

GANPAT UNIVERSITY
INFORMATION TECHNOLOGY
B. TECH. SEMESTER-VI
2CEIT6PE7: ETHICAL HACKING

PRACTICAL – 2

Aim : Labs of Footprinting & Reconnaissance

1. Open Source Information Gathering using Windows Command Line Utilities

A. Do the ping on the any domain and find the following information:

i. Whether the host is alive or not ?

Yes, the host is alive

ii. Find the IP address

IP Address of the host is 157.240.16.174

iii. Round Trip Time

Approximate round trip times in milliseconds:

Minimum = 21ms,

Maximum = 21ms,

Average = 21ms

iv. TTL value

TTL (Time to Live) Value is 55

v. Packet loss statistics

Packets Statistics:

- Sent = 4,
- Received = 4,
- Lost = 0 (0% loss)

Output :

```
C:\Users\Student>ping www.instagram.com

Pinging z-p42-instagram.c10r.instagram.com [157.240.16.174] with 32 bytes of data:
Reply from 157.240.16.174: bytes=32 time=21ms TTL=55
Reply from 157.240.16.174: bytes=32 time=21ms TTL=55
Reply from 157.240.16.174: bytes=32 time=21ms TTL=55
Reply from 157.240.16.174: bytes=32 time=21ms TTL=55

Ping statistics for 157.240.16.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 21ms, Average = 21ms
```

- B. Do Tracert and gather information related to number of hops between source and destination, response time and other related information.

Output :

```
C:\Users\Student>tracert www.yahoo.com

Tracing route to new-fp-shed.wg1.b.yahoo.com [202.165.107.49]
over a maximum of 30 hops:

  1    3 ms    1 ms    3 ms    192.168.24.1
  2   <1 ms   <1 ms   <1 ms   172.16.10.1
  3    3 ms    <1 ms   <1 ms   14.139.122.242
  4   <1 ms    1 ms   <1 ms   10.119.237.53
  5    *      *      *      Request timed out.
  6    *      *      *      Request timed out.
  7   21 ms   21 ms   23 ms   10.152.7.38
  8   26 ms   21 ms   21 ms   115.247.69.85
  9    *      *      *      Request timed out.
 10   *      *      *      Request timed out.
 11   *      *      *      Request timed out.
 12   *      *      *      Request timed out.
 13   81 ms   77 ms   77 ms   ae-5.msr2.sg3.yahoo.com [203.84.209.89]
 14   71 ms   66 ms   66 ms   ae-3.clr1-a-gdc.sg3.yahoo.com [106.10.128.7]
 15   75 ms   78 ms   73 ms   lo0.fab4-3-gdc.sg3.yahoo.com [106.10.131.214]
 16   73 ms   66 ms   73 ms   lo0.usw2-1-lbd.sg3.yahoo.com [106.10.128.247]
 17   74 ms   80 ms   73 ms   media-router-fp73.prod.media.vip.sg3.yahoo.com [202.165.107.49]

Trace complete.
```

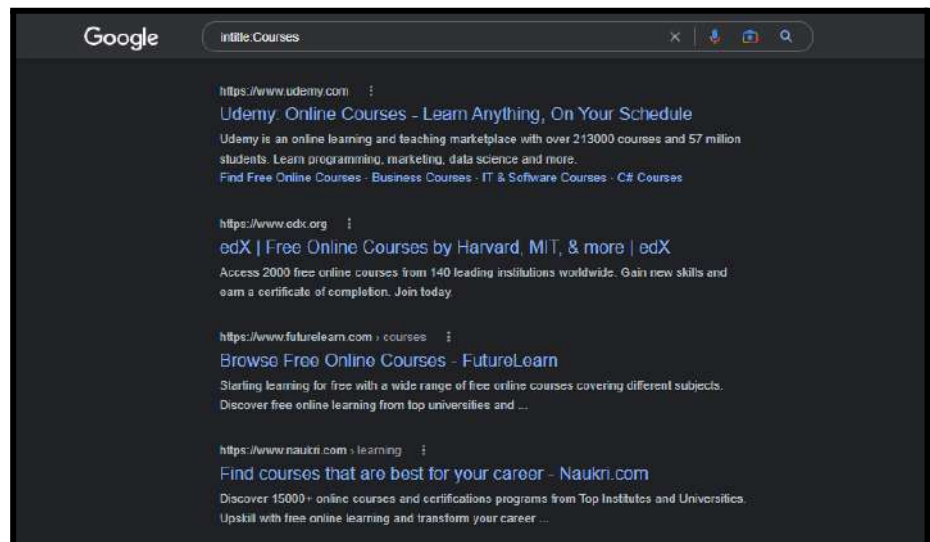
2. Google Hacking Techniques using Dorks

A. Google Search Operators :

i. intitle

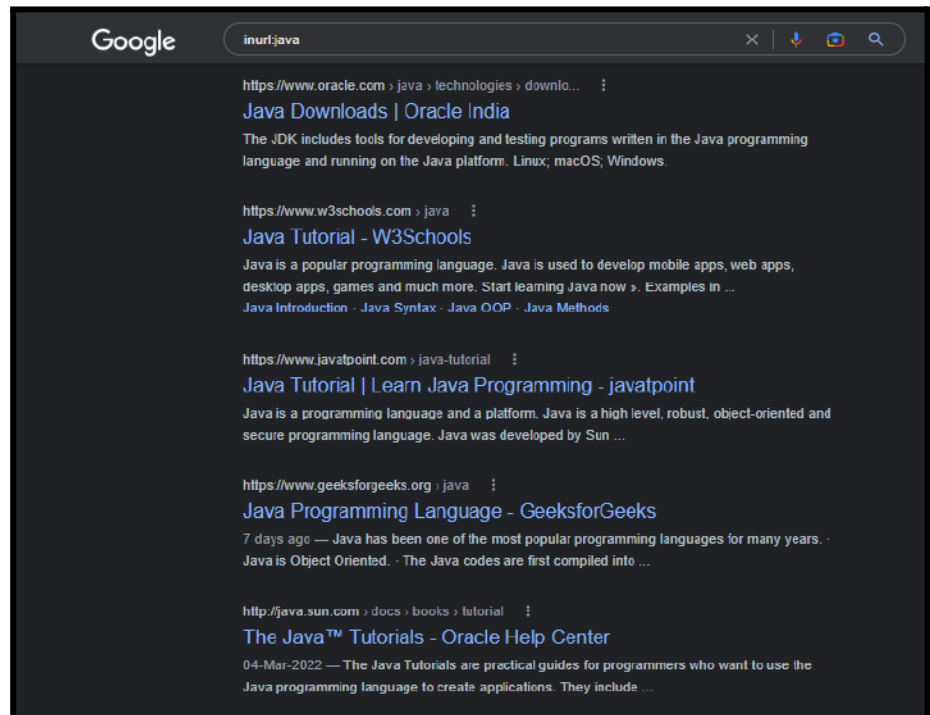
Description : This operator will find web pages with a certain word (or words) in the title.

Output :



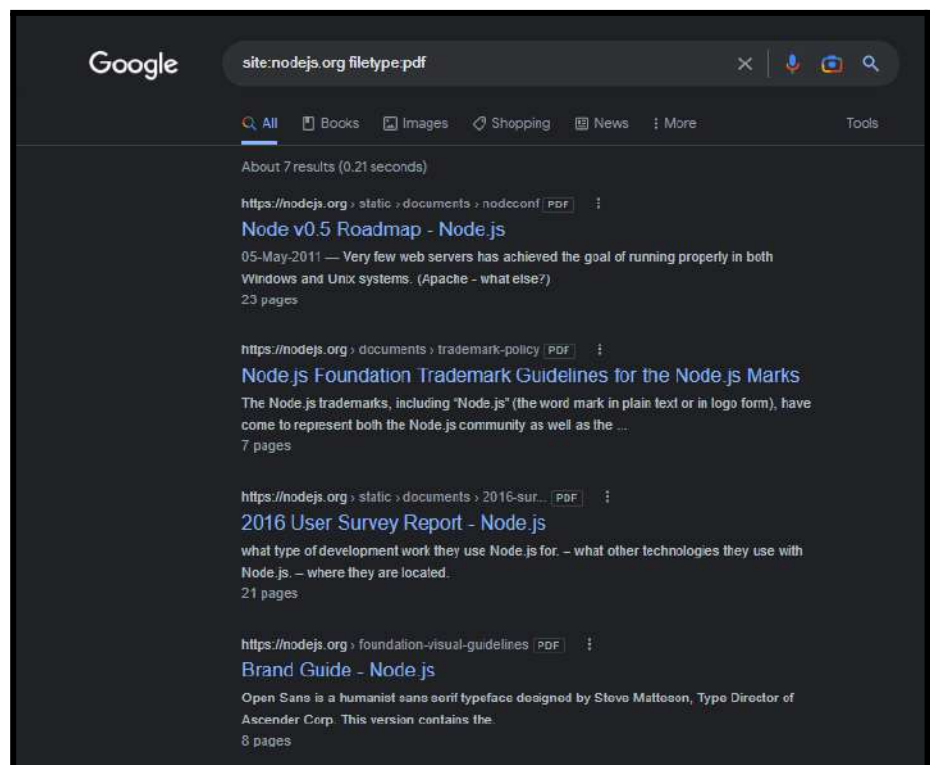
ii. inurl

Description : This operator will find pages with a certain word (or words) in the URL.

Output :

iii. filetype

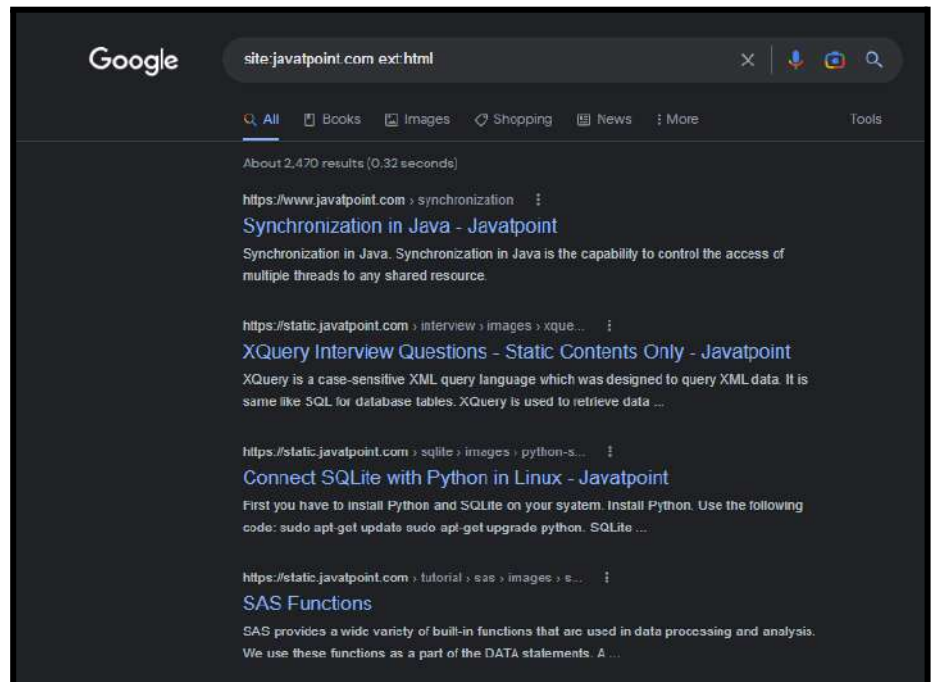
Description : This tool will restrict results to those of a certain filetype. E.g., PDF, DOCX, TXT, PPT, etc.

Output :

iv. ext

Description : This will restrict results to those of a certain filetype. E.g., PDF, DOCX, TXT, PPT, etc. It is same as filetype.

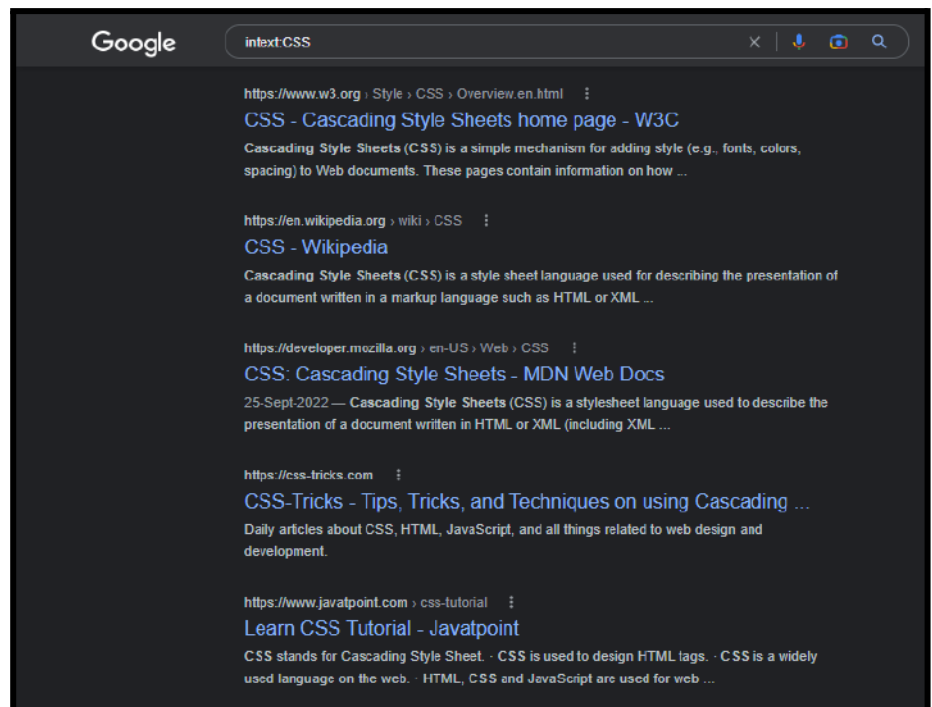
Output :



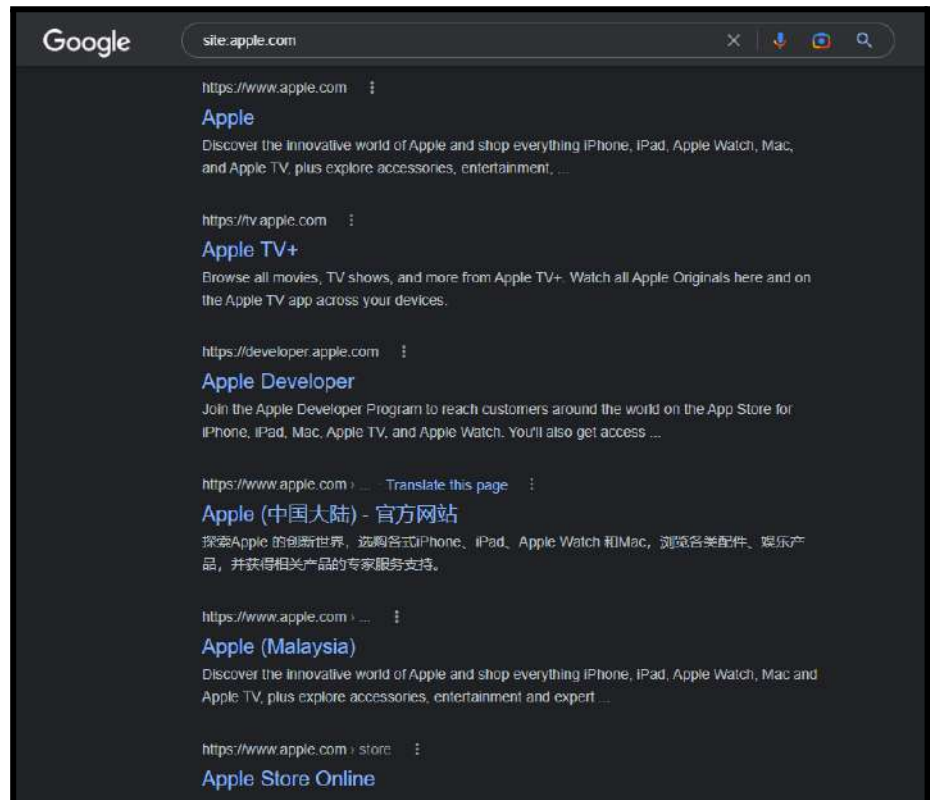
v. intext

Description : This operator will find pages containing a certain word (or words) somewhere in the content.

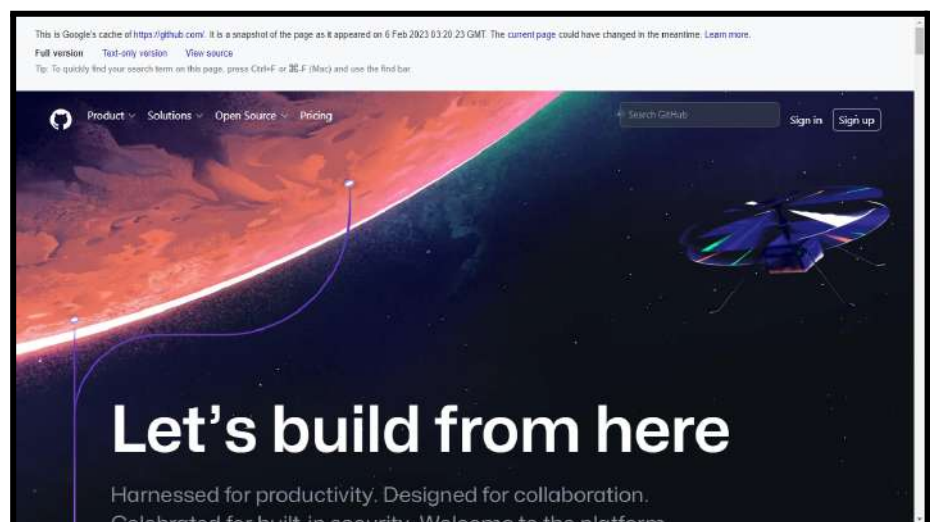
Output :



vi. site

Description : This operator will give results of the specific website only.**Output :**

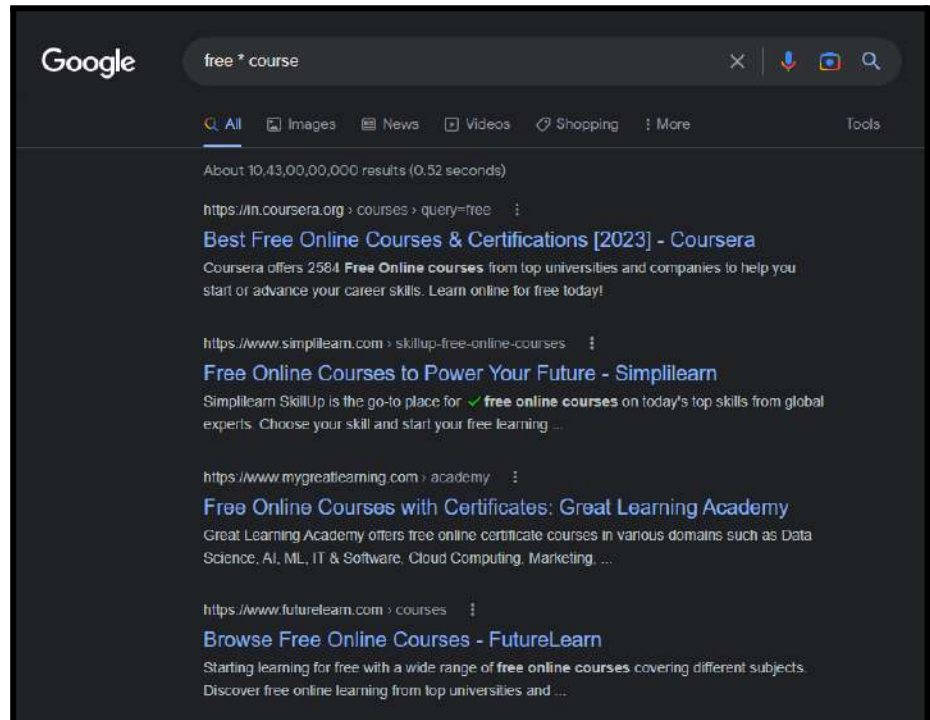
vii. cache

Description : This operator will returns the most recent cached version of a web page**Output :**

viii. *

Description : This is a wildcard and will match any word or phrase

Output :

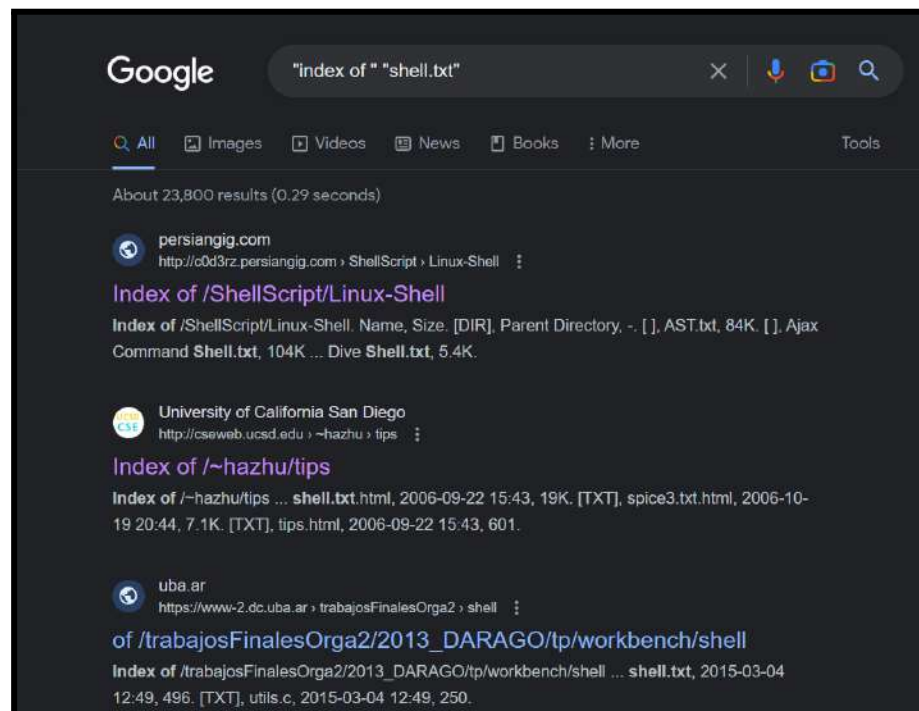


B. Perform any five dorks for the following categories :

i. Files Containing Usernames

Dork 1 : "index of " "shell.txt"

Output :



Index of ~/hazhu/tips

Name	Last modified	Size	Description
Parent Directory	-	-	-
adder.txt.html	2006-09-22 15:42	7.4K	
admin.txt.html	2006-09-22 15:42	3.5K	
ccpp.txt.html	2006-09-22 15:42	5.4K	
cvs.txt.html	2006-09-22 15:42	18K	
cvs_cheat_sheet.txt.html	2006-10-16 13:50	22K	
cvs_how_to.txt.html	2006-10-16 13:47	15K	
hspice.txt.html	2006-09-22 15:42	3.5K	
latex.txt.html	2006-09-22 15:43	4.1K	
linux.txt.html	2006-12-12 16:11	30K	
modelsim.txt.html	2006-10-19 20:44	4.0K	
ms.txt.html	2006-09-22 15:43	429	
perl.txt.html	2006-09-22 15:43	4.2K	
security.txt.html	2006-09-22 15:43	3.1K	
shell.txt.html	2006-09-22 15:43	19K	
spice3.txt.html	2006-10-19 20:44	7.1K	
tips.html	2006-09-22 15:43	601	
verilog.txt.html	2006-12-03 11:35	15K	
vhdl.txt.html	2006-09-22 15:43	16K	
vim.txt.html	2006-11-13 22:57	12K	
vuc.txt.html	2006-09-22 15:43	4.5K	

Apache/2.4.29 (Ubuntu) Server at cseweb.ucsd.edu Port 443

Dork 2 : intitle:"index of" "database.sql"

Output :

Google search results for intitle:"index of" "database.sql"

nuticious
http://www.nuticious.in › sql
Index of /sql
Index of /sql ; database.sql, 2019-07-17 18:34, 821K.

149.54.26
http://149.54.26.73
Index of /
Name · Last modified · Size · Description. [DIR], complaints/, 2023-02-23 05:47, -, [], database.sql, 2022-12-27 04:23, 0, [], db.sql, 2022-12-27 04:41 ...

Apple.Pro
http://apple.pro › Packages
Index of /Packages/
Directory themes, 2015-04-27 17:13, -, [CMP] database.sql.zip, 2015-04-27 17:12, 392k. [TXT] home_alternative_slideshow.txt, 2015-04-27 17:12, 344k.

ub.gov.mn
https://environment.ub.gov.mn › database › SQL
Index of /database/SQL

Index of /Packages/

Filter Name

Name	Last Modified	Size
Parent Directory		
libraries	2015-04-27 17:12	-
modules	2015-04-27 17:12	-
profiles	2015-04-27 17:13	-
themes	2015-04-27 17:13	-
database.sql.zip	2015-04-27 17:12	392k
home_alternative_slideshow.txt	2015-04-27 17:12	344k
home_basic_slideshow.txt	2015-04-27 17:12	224k
home_product_slideshow.txt	2015-04-27 17:12	608k
home_slider_slideshow.txt	2015-04-27 17:12	676k
home_slideshow.txt	2015-04-27 17:12	820k
Shoot-MultiPurposeDrupalTheme-2014-11-27T18:16-21.mysql	2015-04-27 17:12	3452k

Dork 3 : `intext:"index of" ".git"`

Output :

Google `intext:"index of" ".git"`

All Images News Videos Books More Tools

About 14,900 results (0.30 seconds)

High Street Consulting
<https://highstreetconsulting.com> › .git

Index of /.git
 Index of /.git. Name · Last modified · Size · Description · Parent Directory, -. COMMIT_EDITMSG, 2018-03-22 19:25, 15. HEAD, 2017-05-05 14:42, 23.

chlife-stat.org
<https://www.chlife-stat.org> › .git

Index of /.git
 Index of /.git. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [], HEAD, 2023-03-01 08:18, 23. [DIR] ...

nissangdl.mx
<https://nissangdl.mx> › .git

Index of /.git
 Index of /.git. Parent Directory · FETCH_HEAD · HEAD · ORIG_HEAD · branches/ · config · description · hooks/ · index · logs/ · objects/ · packed-refs ...

Index of /.git

Name	Last modified	Size	Description
Parent Directory		-	
COMMIT_EDITMSG	2018-03-22 19:25	15	
HEAD	2017-05-05 14:42	23	
branches/	2017-05-05 14:42	-	
config	2017-05-05 15:01	275	
description	2017-05-05 14:42	73	
hooks/	2017-05-05 14:42	-	
index	2019-01-22 13:50	20K	
info/	2017-05-05 14:42	-	
logs/	2017-05-05 14:58	-	
objects/	2018-03-22 19:25	-	
refs/	2017-05-05 15:01	-	


Dork 4 : `intext:"index of" "phpinfo"`

Output :

Index of /phpinfo

Name	Last modified	Size	Description
Parent Directory		-	
phpinfo.php	2016-06-21 14:37	20	

Apache/2.4.29 (Ubuntu) Server at plataformas.datasisistemasweb.com Port 443

PHP Version 5.6.40-39+ubuntu18.04.1+deb.sury.org+1	
	
System	Linux databaseos 4.15.0-197-generic; #208-Ubuntu SMP Tue Nov 14 17:23:37 UTC 2022 x86_64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/5.6/fpm
Loaded Configuration File	/etc/php/5.6/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/5.6/fpm/conf.d
Additional .ini files parsed	/etc/php/5.6/fpm/conf.d/10-mysqld.ini, /etc/php/5.6/fpm/conf.d/10-opcache.ini, /etc/php/5.6/fpm/conf.d/10-pdo.ini, /etc/php/5.6/fpm/conf.d/15-xml.ini, /etc/php/5.6/fpm/conf.d/20-calendar.ini, /etc/php/5.6/fpm/conf.d/20-ctype.ini, /etc/php/5.6/fpm/conf.d/20-curl.ini, /etc/php/5.6/fpm/conf.d/20-dom.ini, /etc/php/5.6/fpm/conf.d/20-exif.ini, /etc/php/5.6/fpm/conf.d/20-fileinfo.ini, /etc/php/5.6/fpm/conf.d/20-ftp.ini, /etc/php/5.6/fpm/conf.d/20-gd.ini, /etc/php/5.6/fpm/conf.d/20-gettext.ini, /etc/php/5.6/fpm/conf.d/20-iconv.ini, /etc/php/5.6/fpm/conf.d/20-imagick.ini, /etc/php/5.6/fpm/conf.d/20-ldap.ini, /etc/php/5.6/fpm/conf.d/20-mbstring.ini, /etc/php/5.6/fpm/conf.d/20-mysql.ini, /etc/php/5.6/fpm/conf.d/20-mysqli.ini, /etc/php/5.6/fpm/conf.d/20-pdo_mysql.ini, /etc/php/5.6/fpm/conf.d/20-phar.ini, /etc/php/5.6/fpm/conf.d/20-posix.ini, /etc/php/5.6/fpm/conf.d/20-readline.ini, /etc/php/5.6/fpm/conf.d/20-shmop.ini, /etc/php/5.6/fpm/conf.d/20-simplexml.ini, /etc/php/5.6/fpm/conf.d/20-sockets.ini, /etc/php/5.6/fpm/conf.d/20-sqlite3.ini, /etc/php/5.6/fpm/conf.d/20-sysvmsg.ini, /etc/php/5.6/fpm/conf.d/20-sysvsem.ini, /etc/php/5.6/fpm/conf.d/20-sysvshm.ini, /etc/php/5.6/fpm/conf.d/20-tokenizer.ini, /etc/php/5.6/fpm/conf.d/20-wddx.ini, /etc/php/5.6/fpm/conf.d/20-xmlreader.ini, /etc/php/5.6/fpm/conf.d/20-xmlwriter.ini, /etc/php/5.6/fpm/conf.d/20-xsl.ini, /etc/php/5.6/fpm/conf.d/20-zip.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226.NTS
PHP Extension Build	API20131226.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, ssh2.ssh2, ssh2.exec, ssh2.tunnel, ssh2.scp, ssh2.sftp, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv2, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert*, consumed, dechunk, convert.iconv*

Dork 5 : intitle:"index of" "*"db.sh"

Output :

Google search results for the query "intitle: 'index of' '*db.sh'". The search returned approximately 111 results in 0.66 seconds. The top results are:

- Massachusetts Institute of Technology** (https://stuff.mit.edu) - mysql-3.23.6-alpha - sql-bench. The administrators of this directory are Index of /afs/athena/staff/project/databases/mysql/mysql-3.23.6-alpha/sql-bench. This content is being served through the AFS server hector.
- winnergroup.co.th** (https://www.winnergroup.co.th) - files - system - www-. Index of /files/cache/system/db/www-.sh. [ICO], Name - Last modified - Size - Description. [PARENTDIR], Parent Directory, -
- University of Colorado Colorado Springs** (http://cs.uccs.edu) - tinyos - net - tinyos - task - tasksvr. Index of /~cs526/tinyos/tools/java/net/tinyos/task/tasksvr

The bottom of the screenshot shows a table with columns: Name, Last modified, and Size. The table lists the following items:

Name	Last modified	Size
Parent Directory	-	-
MakeInclude	13-Jul-2012 13:30	351
/stuff.mit.edu/afs/athena/staff/project/databases/mysql/mysql-3.23.6-alpha/sql-benc...	3:30	44

Index of /afs/athena/astaff/project/databases/mysql/mysql-3.23.6-alpha/sql-bench

This content is being served through the [AFS](#) server [hector.mit.edu](#) in the [athena.mit.edu AFS cell](#). If you have any questions about this content, please contact the administrators of the [stuff.mit.edu AFS gateway](#) are not responsible for this content and have no ability to remove it.

The administrators of this directory are [dtk.yandros](#) of [athena.mit.edu](#).

Name	Last modified	Size
Parent Directory		-
Data	1999-11-15 11:26	-
Results-linux	1999-07-03 20:46	-
Results-win32	1999-03-08 21:24	-
Results	1999-09-27 17:12	-
limits	1998-09-03 09:28	-
ChangeLog	1998-08-16 08:54	567
Makefile.am	1999-02-28 16:00	2.1K
Makefile.in	1999-11-15 11:26	9.2K
README	1997-11-27 15:51	4.2K
bench-mit.pl.sh	1999-11-15 10:59	11K
compare-results.sh	1999-11-15 10:59	15K
copy-db.sh	1999-11-15 10:59	8.8K
crashme.sh	1999-11-15 10:59	86K
run-all-tests.sh	1999-11-15 10:59	5.8K
server.sfr.sh	1999-11-15 10:59	69K
test-ATIS.sh	1999-11-15 10:59	23K
test-alter-table.sh	1999-11-15 10:59	3.9K
test-bjz-tables.sh	1999-11-15 10:59	3.2K
test-connect.sh	1999-11-15 10:59	7.0K

ii. Files Containing Usernames

Dork 1 : intitle:"index of" "/"usernames"

Output :

Google search results for the query: `intitle:"index of" "/"usernames"`

About 11,900 results (1.04 seconds)

loyce.club
<https://loyce.club/usernames>







Index of /usernames - loyce.club
 Index of /usernames ; [PARENTDIR], Parent Directory, -
 You've visited this page 2 times. Last visit: 31/3/23

People also search for

- [index of /password.txt/ facebook](#)
- [index of /es username and password](#)
- [index of ssn txt](#)
- [index of bitcoin password](#)
- [index of credit card txt 2020](#)
- [cvv2 index of txt rtf](#)

Arista Networks
[https://wiki.edge.arista.com/images/thumb/archive/e/e8/20180612221845!1200x800_reports_web-filter_top-usernames-\(by-size\).png](https://wiki.edge.arista.com/images/thumb/archive/e/e8/20180612221845!1200x800_reports_web-filter_top-usernames-(by-size).png) ; [PARENTDIR], Parent Directory ; [IMG], 120px- ...

Index of /usernames

Name	Last modified	Size	Description
 Parent Directory		-	
 BBCCode.lastday.txt	2023-03-31 10:09	1.4K	
 BBCCode.txt	2023-03-31 10:09	302M	
 note.txt	2020-11-21 10:05	33	
 usernames.lastday.txt	2023-03-31 10:09	309	
 usernames.txt	2023-03-31 10:09	66M	

Apache/2.4.29 (Ubuntu) Server at loyce.club Port 443

Dork 2 : intitle:"index of" "contacts.txt"

Output :

Google search results for intitle:"index of" "contacts.txt"

greenend.org.uk
http://www.chiark.greenend.org.uk › doc › contacts

Index of /doc/git/contrib/contacts - Chiark.greenend.org.uk

Name	Last modified	Size
Parent Directory		-
Makefile	2021-03-08 20:36	1.7K
git-contacts	2021-03-08 20:36	4.4K

[View 1 more row](#)

IBIS Open Forum
https://ibis.org › roster › old96

Index of /roster/old96

Name	Last modified	Size
Parent Directory		-
contacts.txt	1997-01-27 15:20	4.3K
roster.txt	1997-01-27 15:15	21K

[View full table](#)

Iowa State University
https://mesonet.agron.iastate.edu › present › 061010_isu

Index of /present/061010_isu

Name	Last modified	Size
Parent Directory		-
abstract.txt	2012-02-09 16:50	765

Index of /roster/old96

Name	Last modified	Size	Description
Parent Directory		-	
contacts.txt	1997-01-27 15:20	4.3K	
roster.txt	1997-01-27 15:15	21K	

Contact People for Free IBIS Models
11/16/96

Note, for several companies including some that are not listed here, local sales offices may be the preferred point of contact to obtain IBIS Models.

Actel Scott Schlachter 955 East Arques Ave. Sunnyvale, CA 94086-4533 (408) 522-4341 scotts@actel.com	(Future IBIS development planned)
Altera Gary Sugita 3 W. Plumeria San Jose, CA 95134 (408) 894-7882 garys@altera.com	(Future IBIS development planned)
AMCC Dick Spehn Tim Thompson 6195 Lusk Boulevard San Diego, CA 92121-2793 (619) 535-6514 dicks@amcc.com timt@amcc.com	Misc. Models Bipolar and PECL BiCMOS

Dork 3 : intitle:index.of "users.db"

Output :

Google search results for the query "intitle:index.of 'users.db'".

Search results include:

- aactechconnect.com**: <http://www.aactechconnect.com/old/old/users/> - Index of /old/old/users/db
- khoyub.com.ua**: <https://khoyub.com.ua/account/base> - Index of /account/base. [ICO], Name - Last modified - Size - Description. [PARENTDIR], Parent Directory, -, [], **users.db**, 2019-05-28 06:18, 6.0K.
- University of Hawaii**: <http://itm-vm.shidler.hawaii.edu/Examples/Database> - Index of /itm352student/Examples/Assignment4/Assignment4_S18/Quihano_Assignment4/Database ; [], **users.db**, 2019-08-02 15:57, 12K ...

Index of /account/base			
Name	Last modified	Size	Description
 Parent Directory			-
 users.db	2019-05-28 06:18	6.0K	


Dork 4 : intitle:"index of" "users.sql"


Output :


Google

[All](#) [News](#) [Images](#) [Videos](#) [Books](#) [More](#) [Tools](#)

About 154 results (0.98 seconds)

 **csusbak.edu**
<https://www.cs.csusbak.edu/~jshafer/final/sqlFiles> [⋮](#)
Index of /~jshafer/3680_S21/final/sqlFiles
 Index of /~jshafer/3680_S21/final/sqlFiles ; setup.sql, 2021-05-02 23:16, 83 ; **users.sql**, 2021-05-02 23:14, 2.9K ...

 **Levy Baptist Church**
<http://levybaptist.com/sql/users> [⋮](#)
Index of /sql/users
 Index of /sql/users ; Parent Directory ; members.sql.php, 2010-03-17 14:03 ; **users.sql.php**, 2010-03-17 14:03 ...

 **abdib.org.br**
https://www.abdib.org.br/indeed_2_1604452660/sql [⋮](#)
Index of /wp-content/uploads/sites/2/isnapshots ...
 Index of /wp-content/uploads/sites/2/isnapshots/indeed_2_1604452660/sql ; [], **users.sql**, 2020-11-03 22:17, 37.

Index of /~jshafer/3680_S21/final/sqlFiles			
Name	Last modified	Size	Description
Parent Directory			-
have.sql	2021-05-02 23:27	1.4K	
messages.sql	2021-05-02 23:12	11K	
project.sql	2021-05-13 20:32	721	
queries.sql	2021-05-02 23:44	299	
send.sql	2021-05-02 23:28	3.3K	
session.sql	2021-05-02 23:22	2.4K	
setup.sql	2021-05-02 23:16	83	
users.sql	2021-05-02 23:14	2.9K	

[Download file viewer](#)

CEECs Department | California State University Bakersfield | SCI Bldg III | (661)654-3082 | <http://www.cs.csusb.edu>

Dork 5 : "index of" "users.frm"

[frm : form files used as MySQL Database format files]

Output :

Google search results for the query "index of" "users.frm". The search returned about 405 results in 0.36 seconds. The top results are from Exploit-DB, knez.club, and 47.99.216.

Exploit-DB
<https://www.exploit-db.com/ghdb>
"index of" "users.frm" - Files Containing Usernames GHDB ...
 14-Sept-2020 — Google Dork: "index of" "users.frm" # Description :- Disclosure of database file tables and sensitive files. # Date: 13/09/2020 # Author: ...

knez.club
<https://knez.club/mysql/website>
Index of /mysql/website
 Index of /mysql/website ... rsvp.MYI, 2010-05-17 20:27, 6.0K. [], rsvp.frm, 2010-02-28 09:18, 8.6K. [], users.frm, 2009-06-13 18:19, 8.5K ...

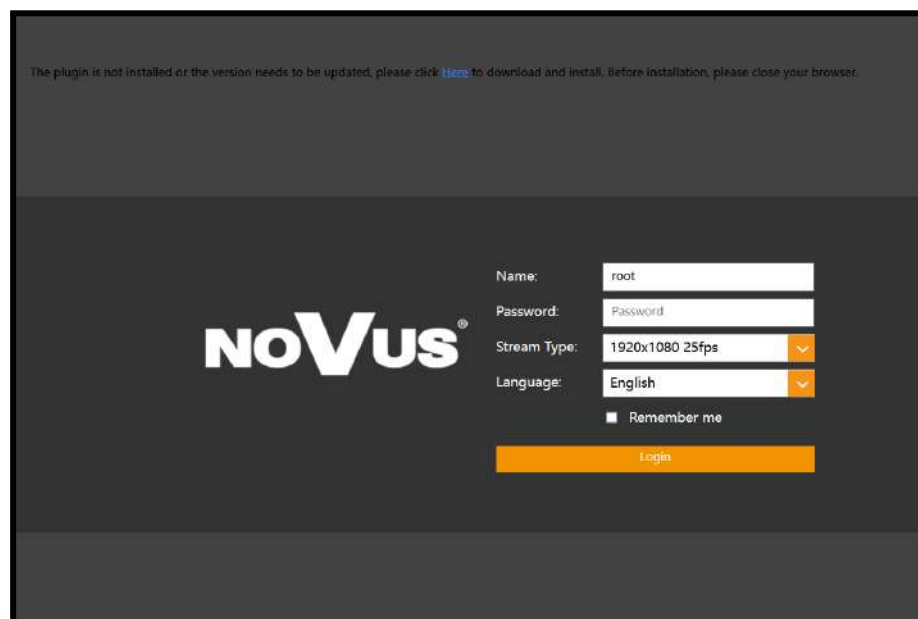
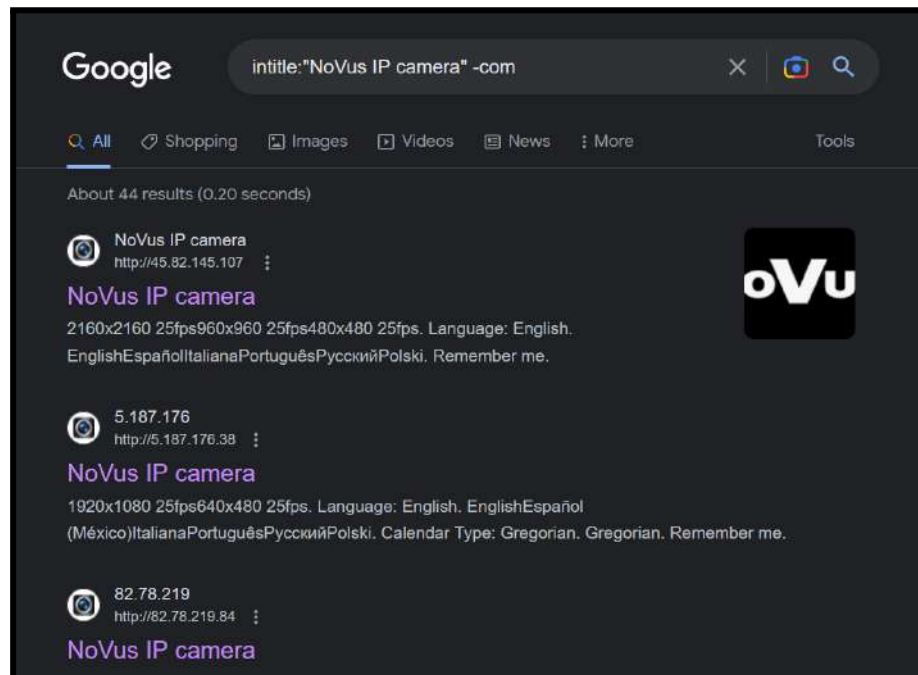
47.99.216
<http://47.99.216.125/mysql/backup/phpmyadmin>
Index of /mysql/backup/phpmyadmin
 Index of /mysql/backup/phpmyadmin ... pma__users.frm, 2015-11-10 23:25, 1.3K. [], pma__users.ibd, 2015-11-10 23:25, 96K ...

Index of /mysql/website

Name	Last modified	Size	Description
Parent Directory		-	
blog.frm	2009-06-13 18:19	8.5K	
blogcategory.frm	2009-06-13 18:19	8.4K	
db.opt	2009-06-13 18:19	65	
feedback.MYD	2011-09-20 03:15	111K	
feedback.MYI	2011-09-20 03:15	119K	
feedback.frm	2009-06-13 18:19	8.5K	
feedback_wedding.MYD	2010-06-02 08:28	3.1K	
feedback_wedding.MYI	2010-06-02 08:28	7.0K	
feedback_wedding.frm	2009-11-07 17:01	8.5K	
groups.frm	2009-06-13 18:19	8.4K	
notebook.frm	2009-06-13 18:19	8.5K	
rsvp.MYD	2010-05-17 20:27	6.3K	
rsvp.MYI	2010-05-17 20:27	6.0K	
rsvp.frm	2010-02-28 09:18	8.6K	
users.frm	2009-06-13 18:19	8.5K	

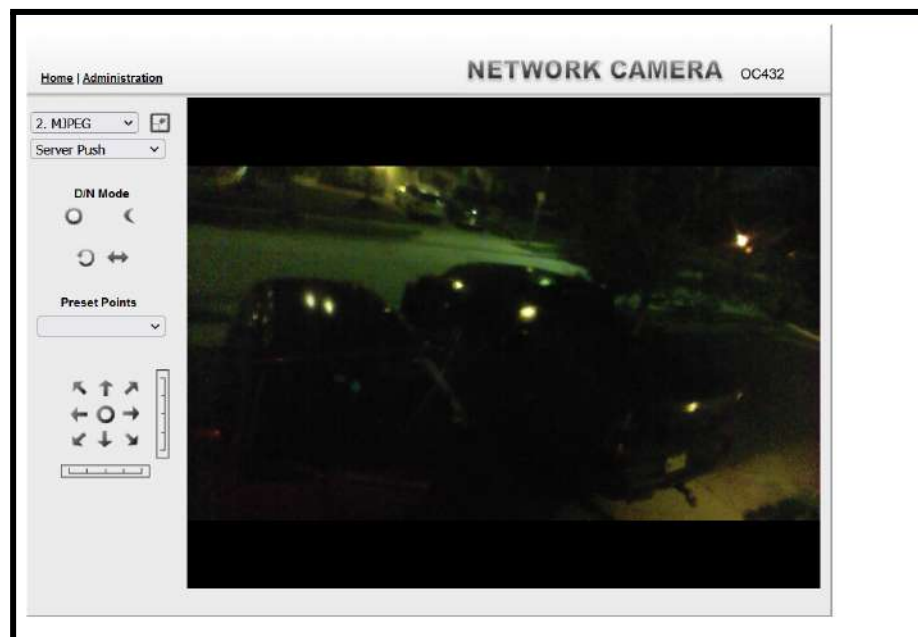
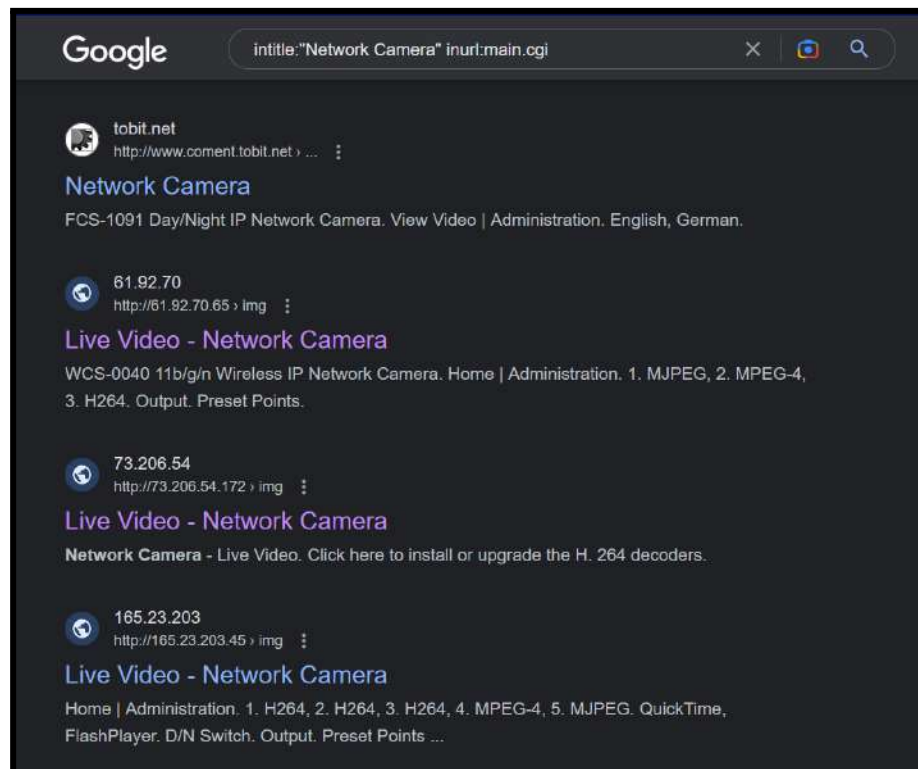
Apache/2.4.52 (Ubuntu) Server at knez.club Port 443

iii. Various Online Devices

Dork 1 : intitle:"NoVus IP camera" -com**Output :**

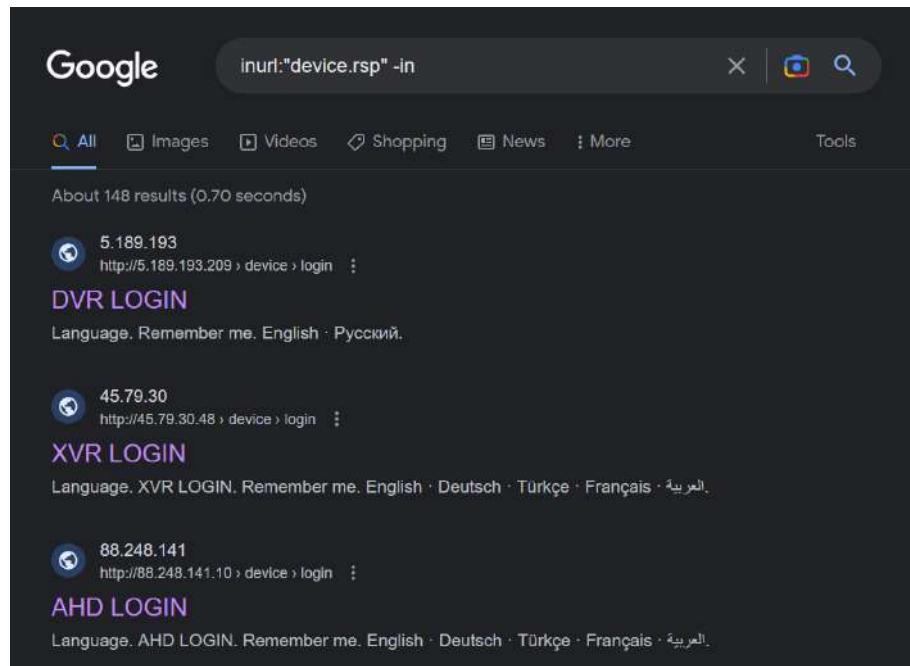
Dork 2 : `intitle:"Network Camera" inurl:main.cgi`

Output :



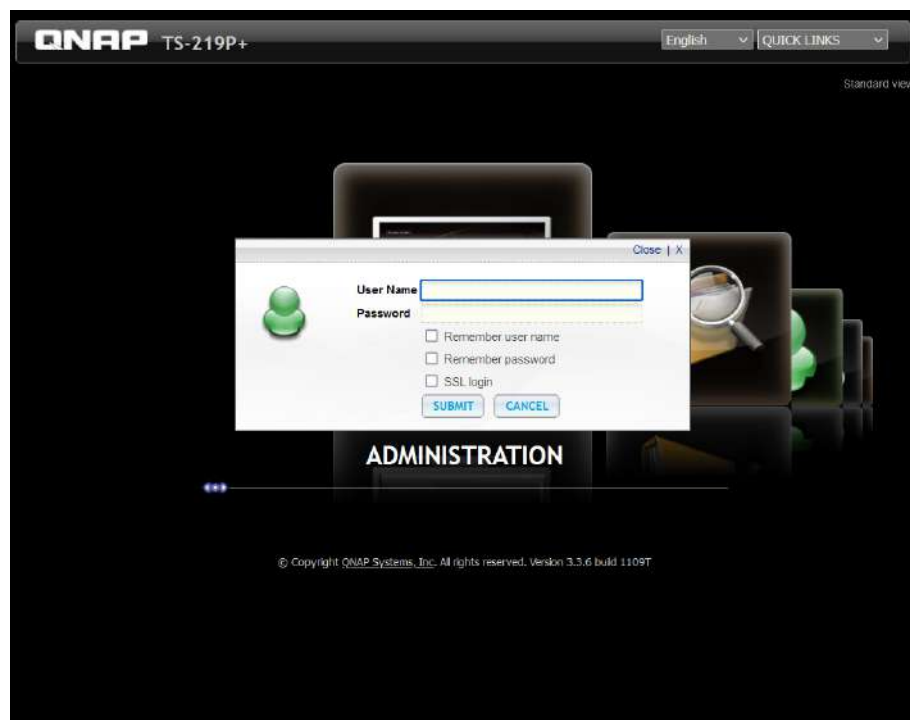
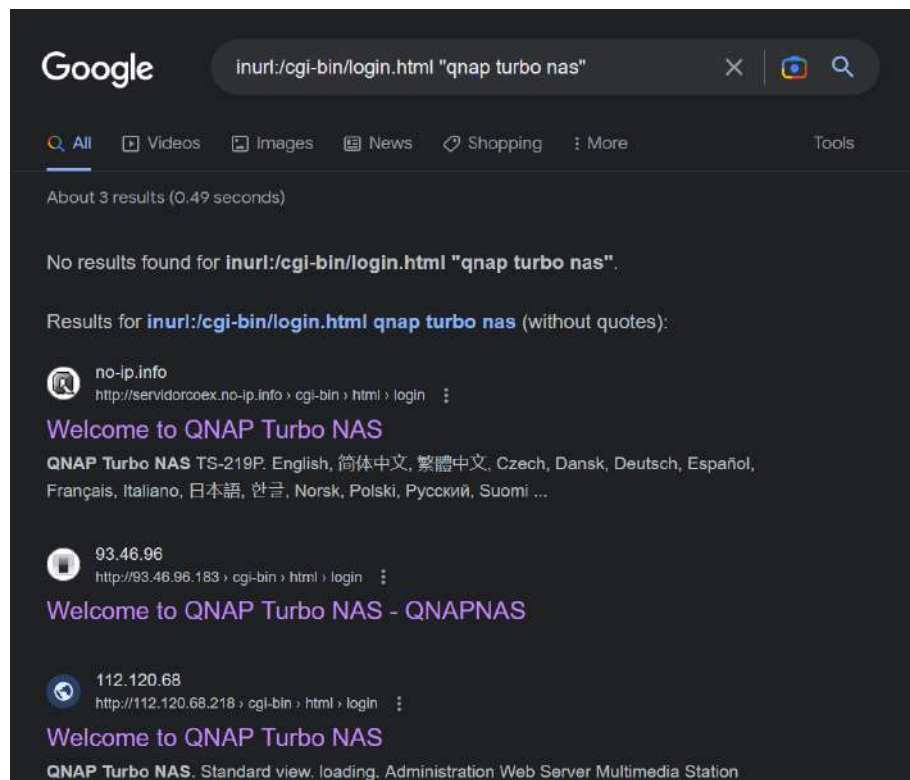
Dork 3 : `inurl:"device.rsp" -in`

Output :



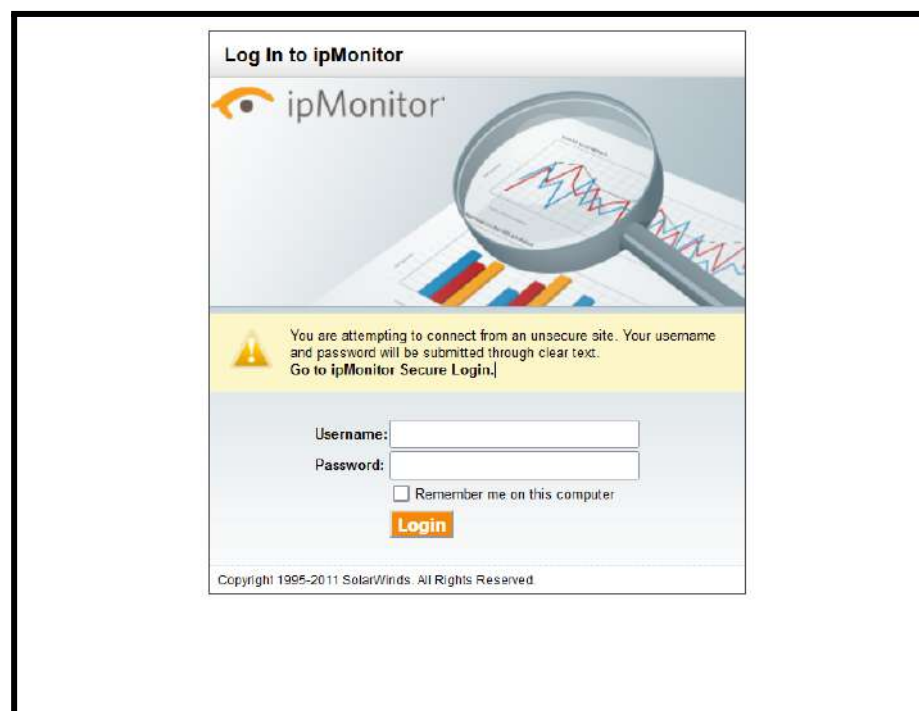
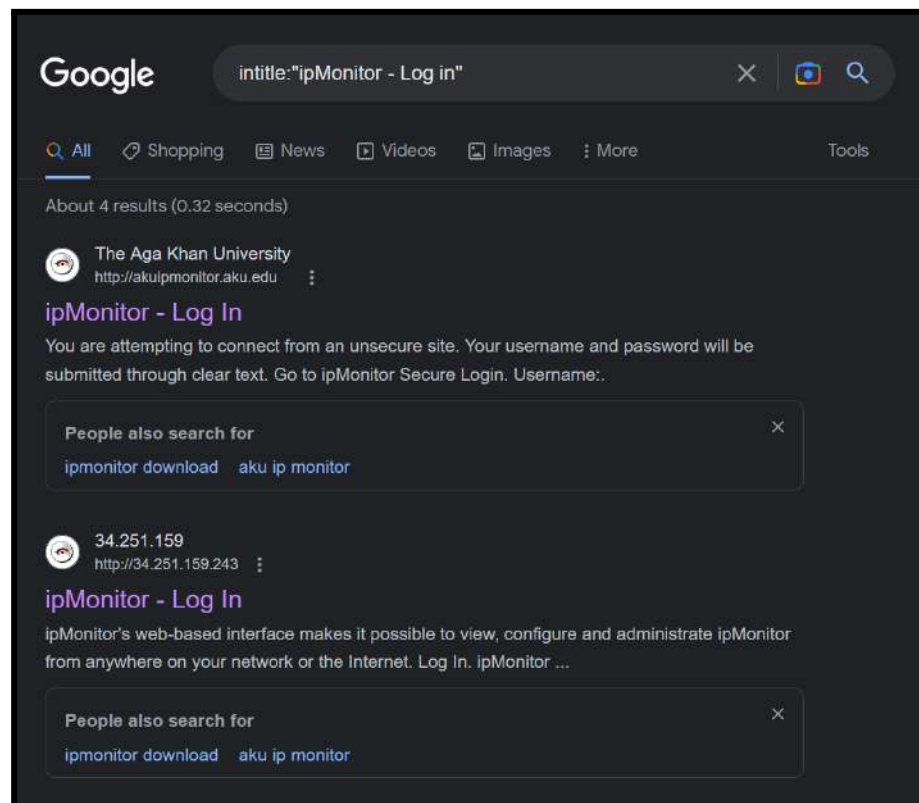
Dork 4 : `inurl:/cgi-bin/login.html "qnap turbo nas"`

Output :



Dork 5 : intitle:"ipMonitor - Log in"

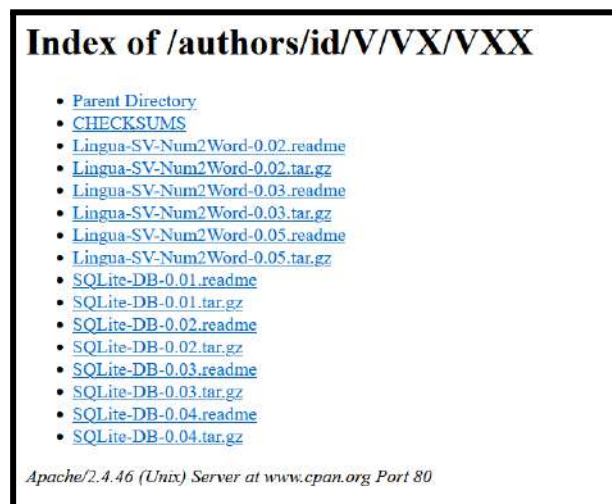
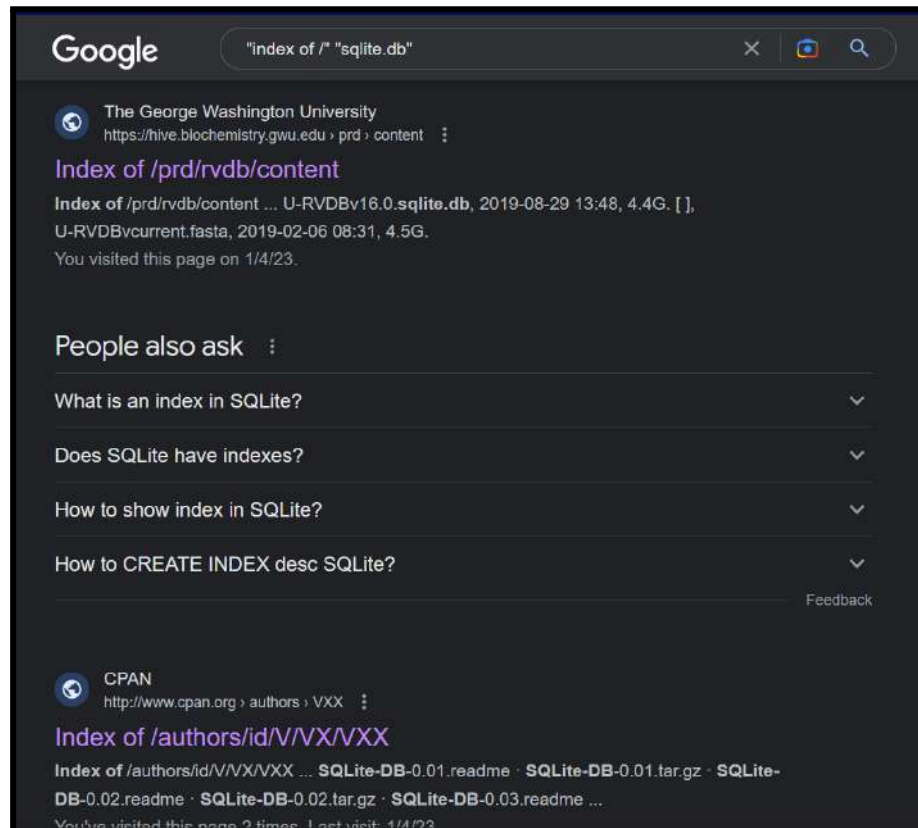
Output :



iv. Sensitive Directories

Dork 1 : intitle:"index of /" "sqlite.db"

Output :



Dork 2 : intitle: "index of" "payment"

Output :

Google

MEDENT
https://www.medent.com › medentvideos › E-Superbil...

of /med_download/medentvideos/v220/E-Superbill Credit ...

Name	Last modified	Size
Parent Directory		-
1_Verifone_Welcome_with edits.png	2018-04-20 17:10	386K
2_Insert_Credit_Card_Prompt.PNG	2018-04-20 17:10	7.4K

[View 31 more rows](#)

PacketFence
https://www.packetfence.org › doc › images › billing

Index of /doc/images/billing

Name	Last modified	Size
Parent Directory		-
authorize-md5-hash.png	08-Mar-2023 09:32	43K
authorize-packetfence-config.png	08-Mar-2023 09:32	332K

[View 14 more rows](#)

General Tommy Franks Leadership Institute and Museum
http://www.store.tommyfranksmuseum.org › payment

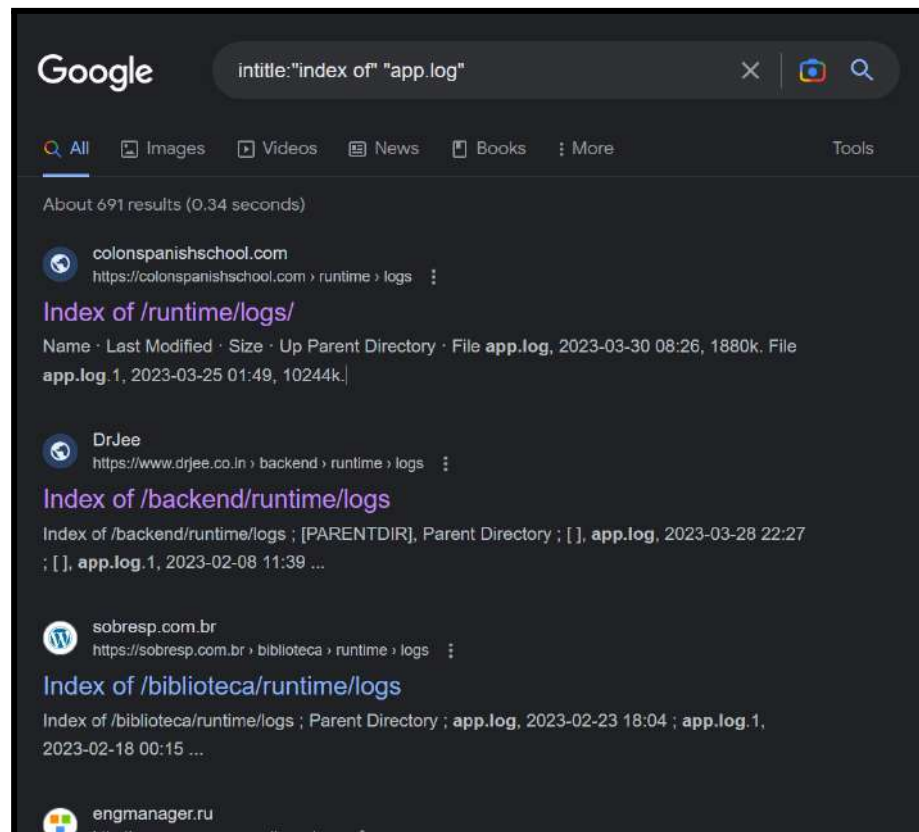
of /payment

Index of /payment ; uc_2checkout/, 2012-05-19 08:40 ; uc_authorizenet/, 2011-05-18 18:27 ; uc_credit/, 2012-05-19 08:40 ...

Index of /med_download/medentvideos/v220/E-Superbill Credit Card				
Name	Last modified	Size	Description	
Parent Directory		-		
1_Verifone_Welcome_with edits.png	2018-04-20 17:10	386K		
2_Insert_Credit_Card_Prompt.PNG	2018-04-20 17:10	7.4K		
3_Transaction_Approved_Color.png	2018-04-20 17:10	6.6K		
3b2_Verifone_Remove_Card_Swipe_with edits.png	2018-04-20 17:10	425K		
4_Receipt_Without_Signature_with edits_1920x1080.PNG	2018-04-20 17:10	105K		
5_Receipt_With_Sign_Here_with edits_1920x1080.PNG	2018-04-20 17:10	106K		
6_Receipt_Signature_with edits no address_with edits_1920x1080.png	2018-04-20 17:10	122K		
8_Receipt_Email_1920x1080.PNG	2018-04-20 17:10	126K		
8_Receipt_Email_with edits_2_1920x1080.png	2018-04-20 17:10	120K		
8_Receipt_Print_1920x1080.PNG	2018-04-20 17:10	17K		
9_ESB_Log_Shows_Payment_Transaction.PNG	2018-04-20 17:10	53K		
Credit Card Payment.png	2018-04-20 17:10	1.0K		
Credit Card Payment Completed.png	2018-04-20 17:10	1.4K		
E-Superbill Credit Card Payment.camproj	2018-04-20 17:10	7.5K		
E-Superbill Credit Card Payment.html	2018-04-20 17:10	839		
E-Superbill Credit Card Payment.mp4	2018-04-20 17:10	14M		
E-Superbill Credit Card Payment.trec	2018-04-20 17:10	19M		
E-Superbill Credit Card Payment.tscproj	2018-04-20 17:10	2.7M		
E-Superbill Credit Card Payment.wav	2018-04-20 17:10	46M		
E-Superbill Credit Card Payment_config.xml	2018-04-20 17:10	2.9K		
E-Superbill Credit Card Payment_embed.css	2018-04-20 17:10	385		
E-Superbill Credit Card Payment_player.html	2018-04-20 17:10	7.1K		
E-Superbill Credit Card Payment_First_Frame.png	2018-04-20 17:10	191K		
E-Superbill Credit Card Payment_Thumbnails.png	2018-04-20 17:10	0		

Dork 3 : intitle:"index of" "app.log"

Output :



Index of /backend/runtime/logs

Name	Last modified	Size	Description
Parent Directory		-	
app.log	2023-03-28 22:27	2.5M	
app.log.1	2023-02-08 11:39	10M	

Apache/2.4.29 (Ubuntu) Server at www.drjee.co.in Port 443

Dork 4 : intitle:"index of" "firewall.log" | "firewall.logs"

Output :

Google search results for the dork: `intitle:"index of" "firewall.log" | "firewall.logs"`

anzalweb.ir
<https://anzalweb.ir/wp-content/uploads/2016/09/>
Index of /wp-content/uploads/2016/09/

Name	Last Modified	Size
security.jpg	2016-09-01 08:26	32k
security-70x46.jpg	2016-09-01 08:26	4k
security-380x120.jpg	2016-09-01 08:26	8k

Camp Rock of Georgia
<https://camprockga.com/wp-content/src/controller>
Index of /wp-content/plugins/wp-defender/src/controller

... 2021-08-30 20:26 12K blocklist-monitor.php 2021-08-30 20:26 5.5K dashboard.php
 2021-08-30 20:26 7.6K firewall-logs.php 2021-08-30 20:26 11K firewall.php ...

rlworkman.net
<https://rlworkman.net/pkgs/sources/11.0/ulogd>
Index of /pkgs/sources/11.0/ulogd - rlworkman.net

ulogd is a handy add-on for netfilter/iptables which allows you to have your **firewall logs** put somewhere besides the main system logs Be sure to check the ...

Index of /wp-content/uploads/2016/09/

Filter Name

Name	Last Modified	Size
Parent Directory		
security.jpg	2016-09-01 08:26	32k
security-70x46.jpg	2016-09-01 08:26	4k
security-380x120.jpg	2016-09-01 08:26	8k
security-164x52.jpg	2016-09-01 08:26	8k
mac-addresses.jpg	2016-09-01 08:38	68k
mac-addresses-310x190.jpg	2016-09-01 08:38	8k
mac-addresses-70x46.jpg	2016-09-01 08:38	4k
mac-addresses-164x101.jpg	2016-09-01 08:38	12k
portforwarding.jpg	2016-09-01 08:51	36k
portforwarding-380x155.jpg	2016-09-01 08:51	8k
portforwarding-70x46.jpg	2016-09-01 08:51	4k
portforwarding-164x67.jpg	2016-09-01 08:51	8k
qos.jpg	2016-09-01 09:14	68k
qos-70x46.jpg	2016-09-01 09:14	4k

#	IPv4 Address	Device Name	MAC Address
1	192.168.0.10	UNKNOWN	
2	192.168.0.16	Andys-Air	
3	192.168.0.20	Windows-Phone	
4	192.168.0.32	PANASONIC TV	
5	192.168.0.4	android-d6b15a186fcc97a8	
6	192.168.0.3	SKY+HD	
7	192.168.0.19	Windows-Phone	
8	192.168.0.3	UNKNOWN	
9	192.168.0.25	android-ababe476e5eda432	
10	192.168.0.29	kindle-cf0cca102	
11	192.168.0.10	UNKNOWN	

Dork 5 : intitle:" index of "/Invoices*"

Output :

Google search results for the query: `intitle:" index of "/Invoices*"`

About 3,710 results (0.35 seconds)

qrbank.net
<https://qrbank.net/invoices>
Index of /invoices/56
 Index of /invoices/56 ; Parent Directory, -.


C.S. Harris
<https://csharris.net/INVOICES>
Index of /INVOICES
 Index of /INVOICES. Name · Last modified · Size · Description · Parent Directory ...

Sambhav Nature Cure Hospital
<https://sambhavcure.com/templates/invoice>
Index of /shopping/wp-content/uploads/woocommerce-pdf- ...
 Index of /shopping/wp-content/uploads/woocommerce-pdf-invoices/templates/invoice. Name · Last modified · Size · Description · Parent Directory, -.

People also search for

- [index of account](#)
- [index of parent directory accounts](#)
- [index of: /services/pancard/](#)

Name	Last modified	Size	Description
Parent Directory		-	
Postpaid_Bill_981082.>	2019-01-05 15:38	244K	

MOBILE SERVICES		airtel	
Original Copy for Recipient - Tax Invoice			
Mr Sneh Goel 502 Prakashdeep Bldg 7 Tolstoy Marg New Delhi 110001 Delhi Landmark:  9810825525 102-100383329		Airtel number 9810825525 Relationship number 102-100383329 Bill number 687762218 Bill date 24-Dec-2018 Bill period 23-Nov-2018 to 12-Dec-2018 Pay by date 11-Jan-2019 Credit limit ₹49,000.00 Security deposit ₹2,500.00 State Code 07 OST No/UN No	
To update your e-mail id, SMS EMAIL <email id> to 121			
As per the Government directive, effective 1-July-17, existing service tax of 15% has been replaced with 18% GST.			
YOUR ACCOUNT SUMMARY		THIS MONTH'S CHARGES	
Previous balance	942.82	Monthly rentals	799.00
Payments	- 942.82	Usage	0.00
Adjustments	- 0.00	One time charges	0.00
This month's charges	+ 942.82	Taxes	143.82
Amount due till			
11-Jan-2019	= 942.82	Total (₹)	942.82
Amount due after		Total : Nine Hundred Forty Two Rupees and Eighty Two Paise Only	
11-Jan-2019	1,060.82		

v. Vulnerable Files

Dork 1 : intitle:"index of" "/"sql" "admin"


Output :

Google


intitle:"index of" "/"sql" "admin"

Q All Images Videos Books News More Tools


About 42,100 results (1.38 seconds)

 The Apache Software Foundation!
<https://doris.apache.org/sql-manual/sql-reference>

Index of /zh-CN/docs/dev/sql-manual/sql-reference/Database- ...
 Index of /zh-CN/docs/dev/sql-manual/sql-reference/Database-Administration-Statements ; [DIR]
 · [DIR] ; ADMIN-CANCEL-REBALANCE-DISK/ · ADMIN-CANCEL-REPAIR/ ; 2023-01- ...

 Package It
<http://www.packageit.co.za/old/Admin/SQL>

Index of /old/DesktopModules/Admin/SQL
 Index of /old/DesktopModules/Admin/SQL ; Parent Directory ; App_LocalResources/
 2013-11-10 13:31 ; SQL.ascx.cs, 2013-09-24 08:47 ...

 cbjdiffusion.fr
<http://mta.cbjdiffusion.fr/sources/admin/sql>

Index of /sources/module/admin sql
 Index of /sources/module/admin sql ; [PARENTDIR], Parent Directory, -.

People also search for

index of sql query index of /admin

Index of /zh-CN/docs/dev/sql-manual/sql-reference/Databa			
Name	Last modified	Size	Description
Parent Directory		-	
ADMIN-CANCEL-REBALANCE-DISK/	2023-04-01 03:22	-	
ADMIN-CANCEL-REPAIR/	2023-04-01 03:22	-	
ADMIN-CHECK-TABLET/	2023-04-01 03:22	-	
ADMIN-CLEAN-TRASH/	2023-04-01 03:22	-	
ADMIN-COPY-TABLET/	2023-04-01 03:22	-	
ADMIN-DIAGNOSE-TABLET/	2023-04-01 03:22	-	
ADMIN-REBALANCE-DISK/	2023-04-01 03:22	-	
ADMIN-REPAIR-TABLE/	2023-04-01 03:22	-	
ADMIN-SET-CONFIG/	2023-04-01 03:22	-	
ADMIN-SET-REPLICA-STATUS/	2023-04-01 03:22	-	
ADMIN-SHOW-CONFIG/	2023-04-01 03:22	-	
ADMIN-SHOW-REPLICA-DISTRIBUTION/	2023-04-01 03:22	-	
ADMIN-SHOW-REPLICA-STATUS/	2023-04-01 03:22	-	
ADMIN-SHOW-TABLET-STORAGE-FORMAT/	2023-04-01 03:22	-	
ENABLE-FEATURE/	2023-04-01 03:22	-	
INSTALL-PLUGIN/	2023-04-01 03:22	-	
KILL/	2023-04-01 03:22	-	
RECOVER/	2023-04-01 03:22	-	
SET-VARIABLE/	2023-04-01 03:22	-	
UNINSTALL-PLUGIN/	2023-04-01 03:22	-	

Dork 2 : intitle:"index of" "stylesheet.css"

Output :

Google search results for the query: `intitle:"index of" "stylesheet.css"`

About 3,860 results (0.28 seconds)

Uhrenworld München
<https://www.uhrenworld.com> › templates › css

[Index of /templates/xt_responsive/css](#)
 Index of /templates/xt_responsive/css. Parent Directory · Template.505.css · Template.css · css.php · mail.css · **stylesheet.css**.

Emblish Online Shopping
<https://www.emblish.in> › catalog › default › stylesheet

[Index of /catalog/view/theme/default/stylesheet/](#)
 webcreationfeatured.css 24-Mar-2016 03:43 4k [HTM] noty.css 13-Dec-2018 11:53 8k [HTM] responsive.css 06-May-2020 05:32 8k [HTM] **stylesheet.css** 17-Dec-2018 ...

University of Washington
<https://depts.washington.edu> › osfaweb › services › css

[Index of /osfaweb/services/workstudy/css](#)
 Index of /osfaweb/services/workstudy/css ; [TXT], layout.css, 2015-07-22 08:29 ; [TXT], **stylesheet.css**, 2015-07-22 08:29 ...

Index of /catalog/view/theme/default/stylesheet/

Name	Last modified	Size
Parent Directory	21-Feb-2023 09:43	-
d_quickcheckout	27-Nov-2018 14:51	-
d_social_login	27-Nov-2018 14:51	-
font	27-Mar-2019 11:52	-
quiz.css	21-Feb-2023 09:43	4k
just_purchased_notification.css	26-Sep-2022 10:36	4k
testimonial.css	27-Sep-2022 05:40	4k
webcreationfeatured.css	24-Mar-2016 03:43	4k
noty.css	13-Dec-2018 11:53	8k
responsive.css	06-May-2020 05:32	8k
stylesheet.css	17-Dec-2018 12:30	16k
styles.css	23-Dec-2022 12:01	48k
animate.css	26-Sep-2022 10:36	72k

Proudly Served by LiteSpeed Web Server at www.emblish.in Port 443

Dork 3 : intitle:"index of" "*.php"

Output :

Google

intitle:"index of" "*.php"

Q All Images Videos News Books More Tools

About 14,50,000 results (0.46 seconds)

ntu.edu.tw
http://ftp.ntu.edu.tw › php

[Index of /php/](#)

Index of /php/ : ../ archive/ 16-Mar-2023 13:50 - backend/ 31-Mar-2023 21:30 - bin/ 08-Dec-2022 18:50 - conferences/ 22-Aug-2022 17:20 - distributions/ ...

SunDun Vending
https://sundun.com › php

[Index of /php](#)

Index of /php : SMTP version/, 2016-12-01 08:47 ; admin/, 2016-12-01 08:47 ; captcha/, 2016-12-01 08:47 ...

Nigeria Police Force
https://www.npf.gov.ng › php

[Index of /php](#)

Name	Last modified	Size
Parent Directory		-
consultation.php	2019-05-23 02:01	1.1K

Index of /php/			
../			
archive/	16-Mar-2023 13:50	-	
backend/	01-Apr-2023 07:30	-	
bin/	08-Dec-2022 18:50	-	
conferences/	22-Aug-2022 17:20	-	
distributions/	14-Mar-2023 20:10	-	
fonts/	21-Jan-2015 10:53	-	
images/	17-Oct-2022 13:30	-	
include/	01-Apr-2023 07:30	-	
is/	14-Dec-2022 11:40	-	
license/	22-Aug-2022 17:00	-	
manual/	13-Oct-2022 10:30	-	
pear/	31-May-2019 16:10	-	
releases/	16-Mar-2023 13:50	-	
security/	22-Aug-2022 17:00	-	
src/	29-Jun-2022 21:30	-	
stats/	31-May-2019 16:10	-	
styles/	21-Feb-2023 15:10	-	
tests/	15-Jul-2022 11:10	-	
ChangeLog-4.php	26-Jul-2021 14:20		253127
ChangeLog-5.php	26-Jul-2021 14:20		814982
ChangeLog-7.php	03-Nov-2022 09:10		436635
ChangeLog-8.php	16-Mar-2023 13:50		149830

Dork 4 : intitle:"index of" "schema.sql"

Output :

Index of /sf_sandbox/data/sql			
Name	Last modified	Size	Description
Parent Directory		-	
schema.sql	2009-05-08 23:08	888	
sqldb.map	2009-05-08 23:08	44	

Dork 5 : intitle:"Index of" site:.in

Output :

Google search results for the dork `intitle:"Index of" site:.in`. The search returned about 1,97,000 results in 0.39 seconds.

Result 1: iitmandi.ac.in
http://students.iitmandi.ac.in/~u_shivateja
Index of /~u_shivateja

Name	Last modified	Size
Parent Directory	-	-
CloudStack.png	2013-05-19 17:49	37K
alert.js	2014-06-01 20:23	10

View 8 more rows

Result 2: uohyd.ac.in
<https://www.uohyd.ac.in/wp-includes/Text>
Index of /wp-includes/Text

Name	Last modified	Size
Parent Directory	-	-
Diff.php	2022-03-22 21:55	13K
Diff/	2022-03-14 06:16	-

Index of /~u_shivateja

Name	Last modified	Size	Description
Parent Directory		-	
CloudStack.png	2013-05-19 17:49	37K	
alert.js	2014-06-01 20:23	10	
cnp/	2012-10-24 23:22	-	
demo.log	2013-10-06 22:54	48K	
e/	2013-01-26 14:14	-	
master.zip	2014-11-08 00:28	956K	
sigma/	2014-10-30 15:51	-	
sql-maven-plugin-1.5.jar	2013-06-25 02:33	67K	
test/	2014-10-11 23:19	-	
whatstoday/	2014-11-11 04:02	-	

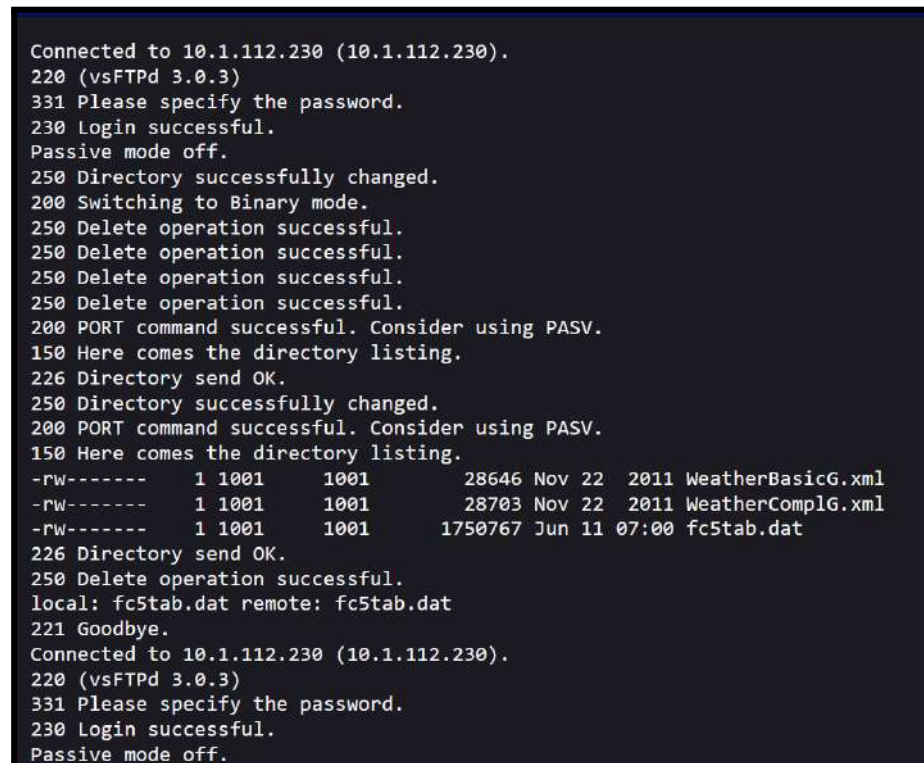
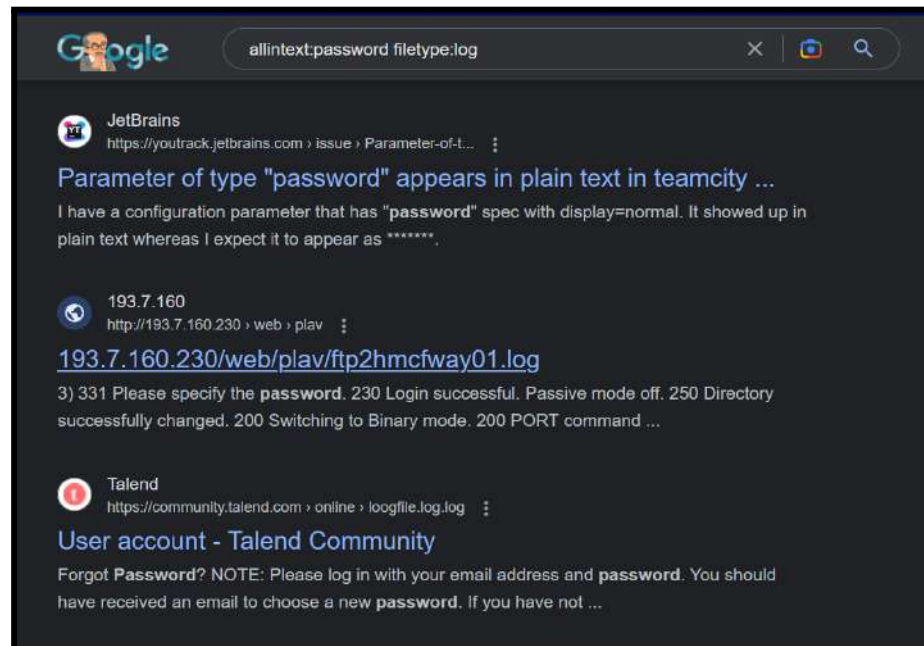
Apache/2.4.18 (Ubuntu) Server at students.iitmandi.ac.in Port 80

C. Write a dorks for the following:

i. Log files for the login credentials

Dork : allintext:password filetype:log

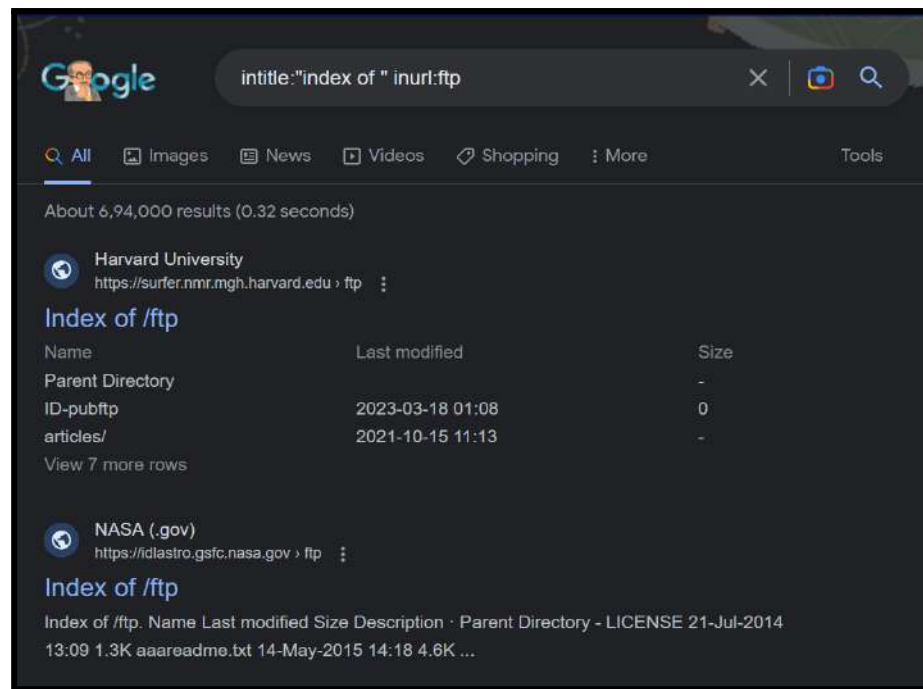
Output :



ii. Open FTP servers

Dork : intitle:"index of " inurl:ftp

Output :

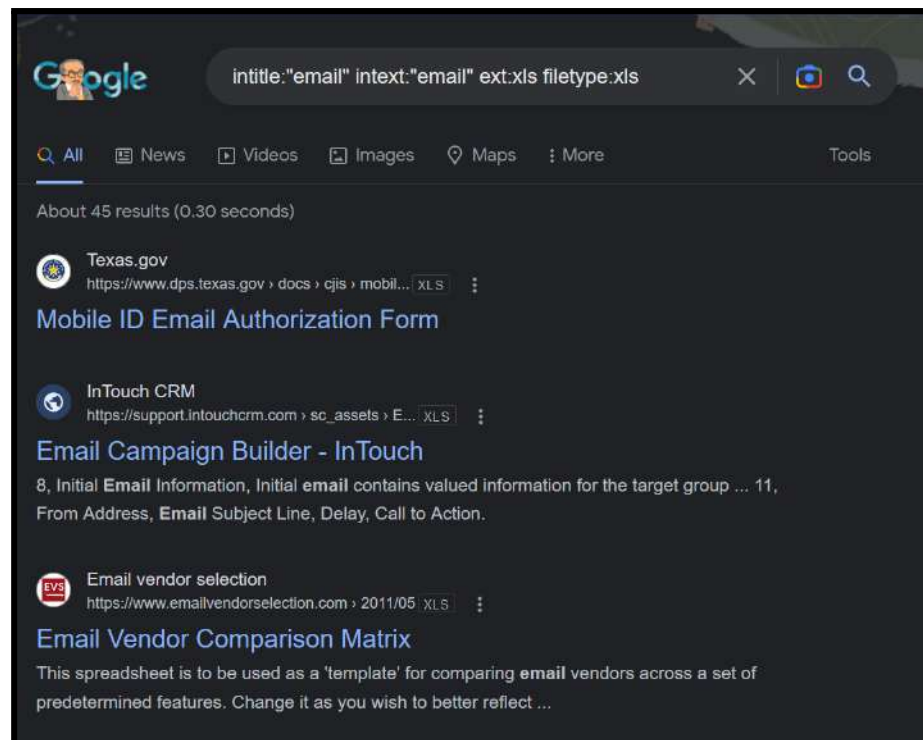


Index of /ftp			
Name	Last modified	Size	Description
Parent Directory		-	
ID-pubftp	2023-03-18 01:08	0	
articles/	2021-10-15 11:13	-	
data/	2023-03-02 01:25	-	
dist/	2022-12-06 13:55	-	
docs/	2022-09-15 10:26	-	
misc/	2006-04-07 15:59	-	
optseq/	2008-08-18 13:47	-	
projects/	2010-09-28 14:15	-	
security/	2004-02-12 18:29	-	

iii. Fetch the excel files containing list if emails

Dork : `intitle:"email" intext:"email" ext:xls filetype:xls`

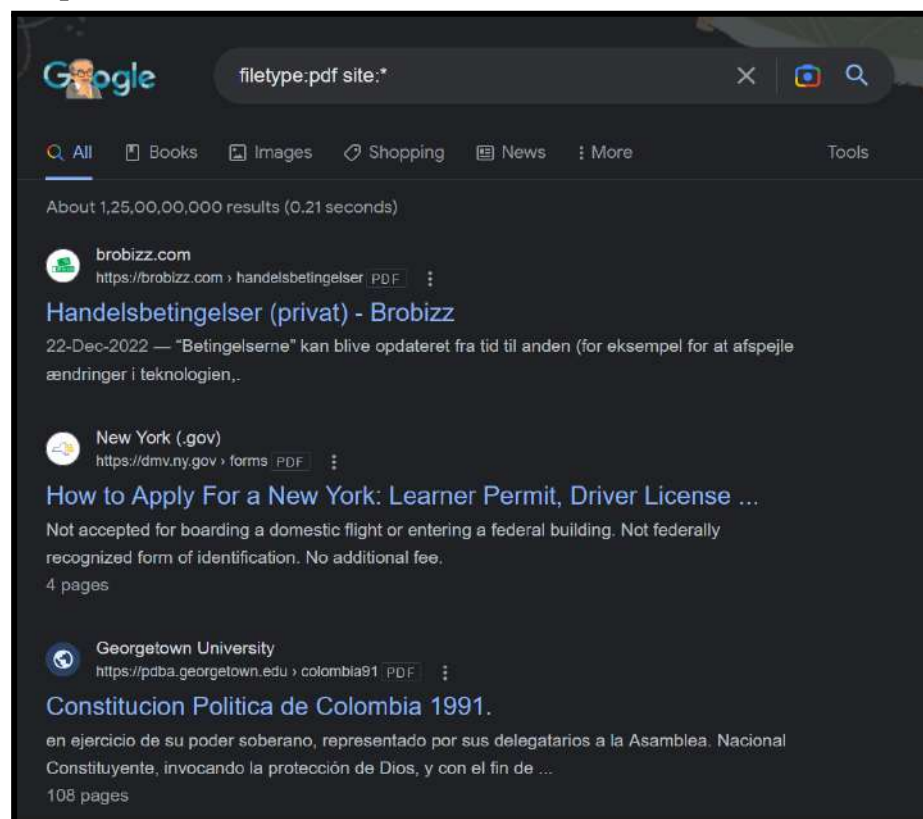
Output :



iv. List only pdf files from the any website

Dork : filetype:pdf site:*

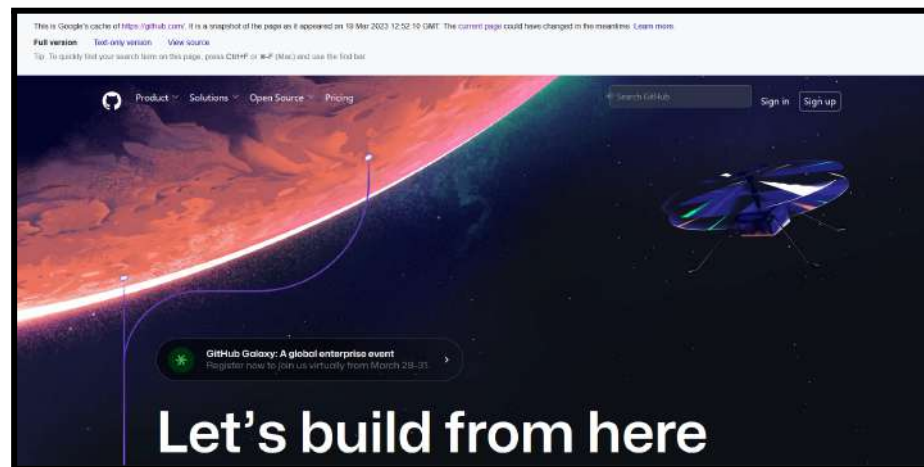
Output :



v. View most recent Cache

Dork : cache:www.github.com

Output :



3. Finding Company's Sub-domains using Sublist3r (Perform in Kali linux)

- Sublist3r helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting over the network.
- It is one of the most widely used tools for enumerating subdomains.
- **Command to Use Sublist3r in kali linux :**
sublist3r -d <domain-name>
 Here, -d is used for Domain Name
- **Command to Use Sublist3r in windows :**
python sublist3r.py -d <domain-name>
 In Windows, we have to run the sublist3r using a python file.
- **Using Sublist3r to find domains of "youtube.com"**

```
PS S:\Ganpat University\GUNI Sem6\Ethical Hacking (EH)\Lab Materials\Programming Files\Sublist3r-master> python sublist3r.py -d google.com

Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for google.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..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 10
www.google.com
account.google.com
admin.google.com
ads.google.com
domains.google.com
home.google.com
myaccount.google.com
search.google.com
support.google.com
workspace.google.com
PS S:\Ganpat University\GUNI Sem6\Ethical Hacking (EH)\Lab Materials\Programming Files\Sublist3r-master>
```

- Using Sublist3r to find domains of "google.com"

```
PS S:\Ganpat University\GUNI Sem6\Ethical Hacking (EH)\Lab Materials\Programming Files\Sublist3r-master> python sublist3r.py -d youtube.com

Sublist3r

# Coded By Ahmed Aboul-Ela - @aboul3la

[+] Enumerating subdomains now for youtube.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..
[!] Error: Virustotal probably now is blocking our requests
[+] Total Unique Subdomains Found: 5
charts.youtube.com
fr.youtube.com
music.youtube.com
tv.youtube.com
tw.youtube.com
PS S:\Ganpat University\GUNI Sem6\Ethical Hacking (EH)\Lab Materials\Programming Files\Sublist3r-master>
```

4. Information Gathering using Maltego

Different Machines available in Maltego for Information Gathering :

Company Stalker :

This Machine will try to get all email addresses tied to a domain and then see which resolves to social networks. It also gets documents and extracts metadata.

Find Wikipedia Edits :

This Machine takes a domain and looks for possible Wikipedia edits.

Footprint Level 1 :

This performs a level 1 (fast, basic) footprint of a domain.

Footprint Level 2 :

This performs a level 2 (mid) footprint of a domain.

Footprint Level 3 :

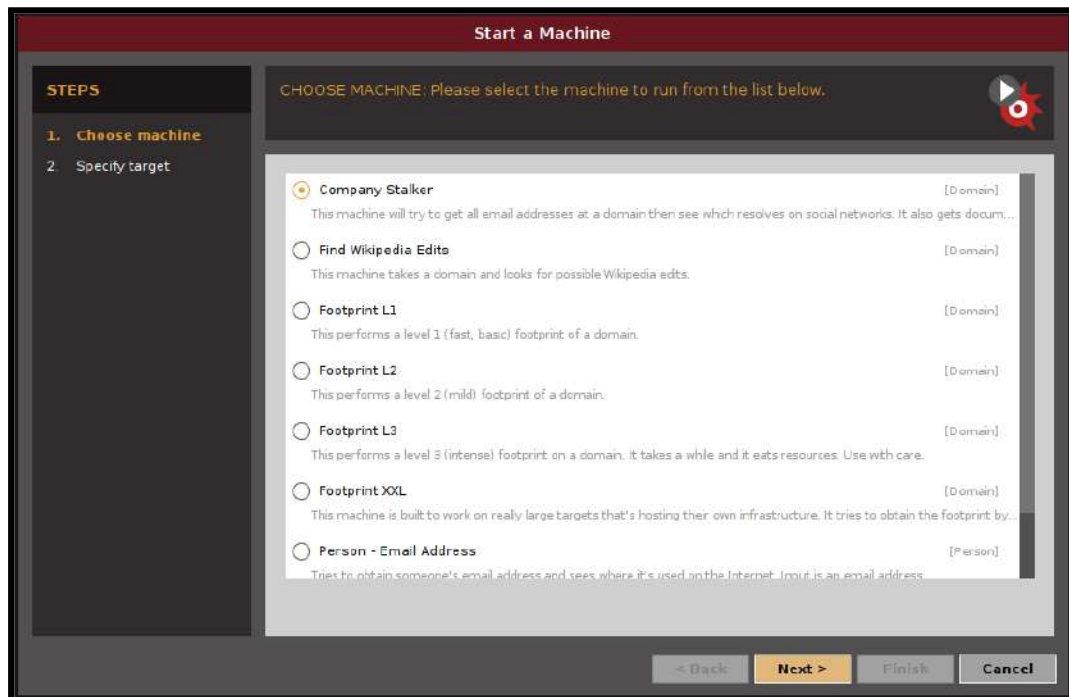
This performs a level 3 (intense) footprint of a domain. It takes a while and eats resources. Use with care.

Footprint XXL :

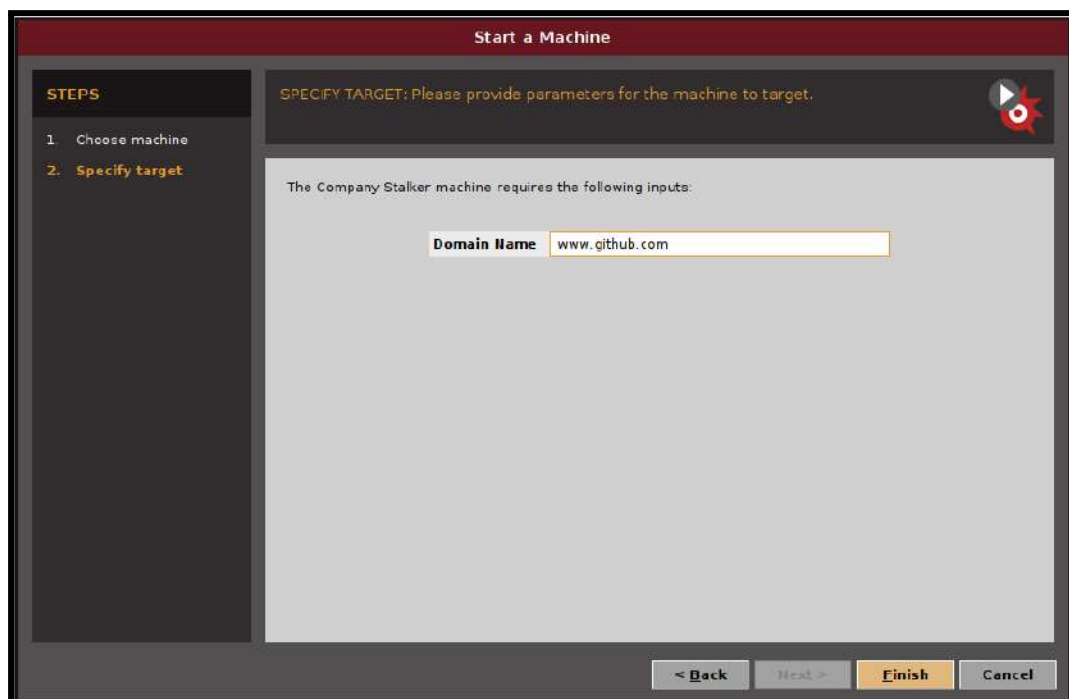
This Machine is built to work on really large targets that are hosting their own infrastructure.

Steps to Start a Machine for Information Gathering [Company Stalker]:

Step 1 : We will choose the Company Stalker machine that we will use.



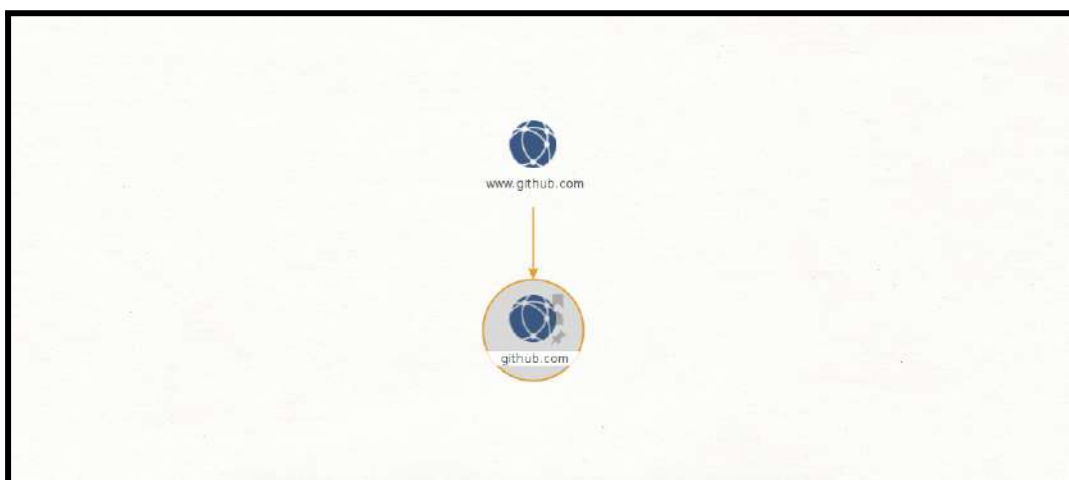
Step 2 : We will define our target domain name



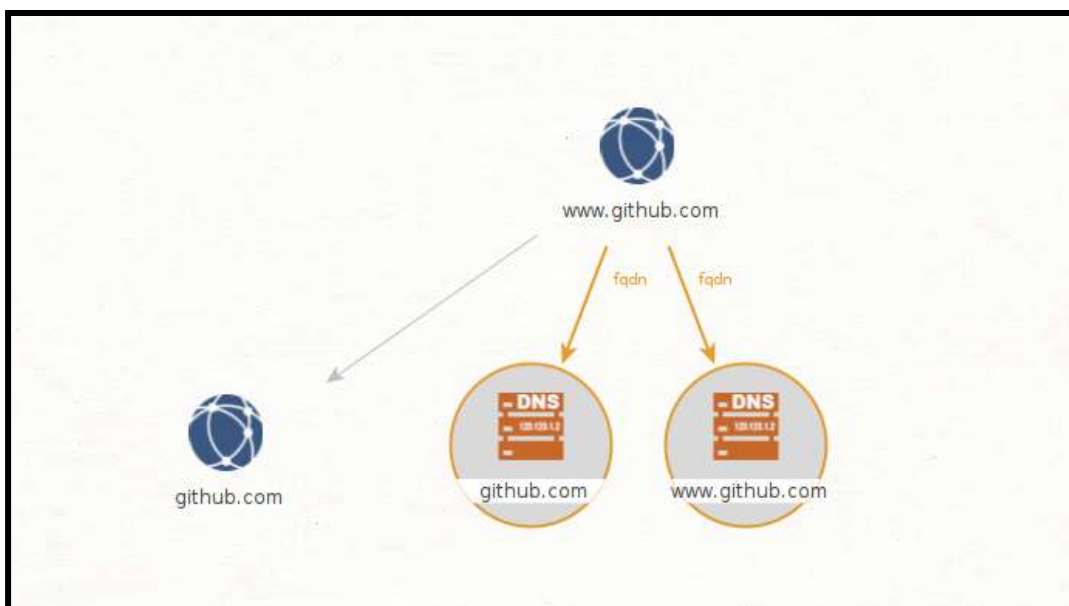
Step 3 : We will get the following graph for the given Domain



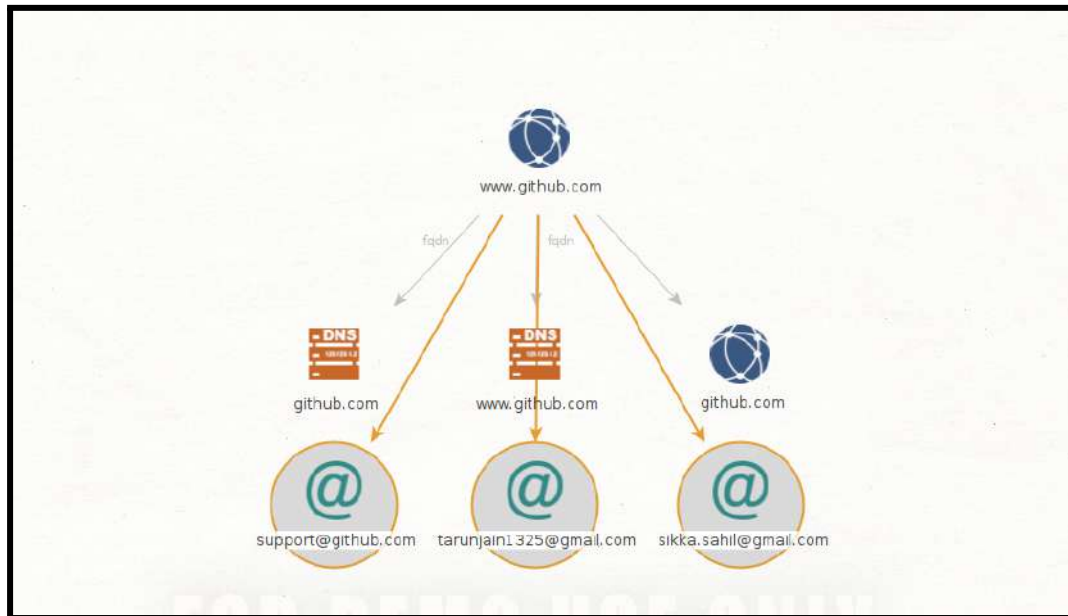
When search for Domains of www.github.com :



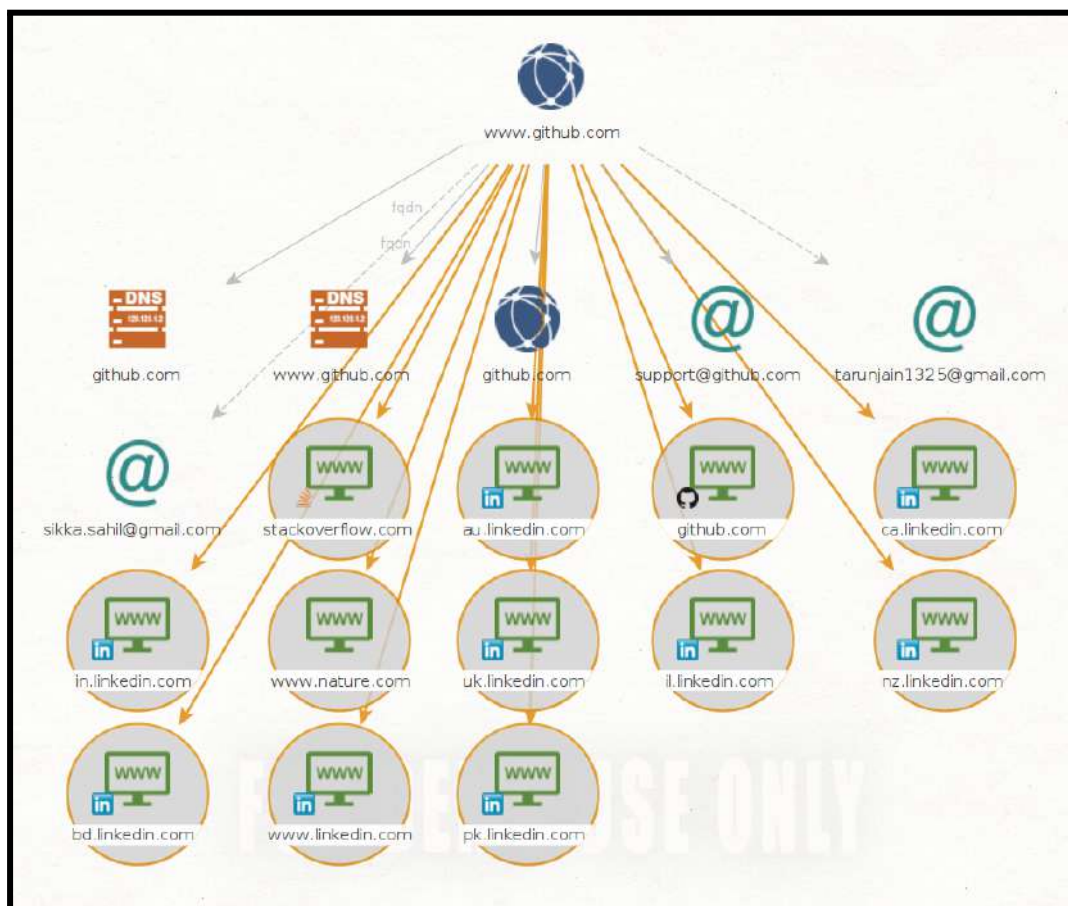
When we Search for DNS Names :



When we Search for Email Address [using Search Engines] on www.github.com

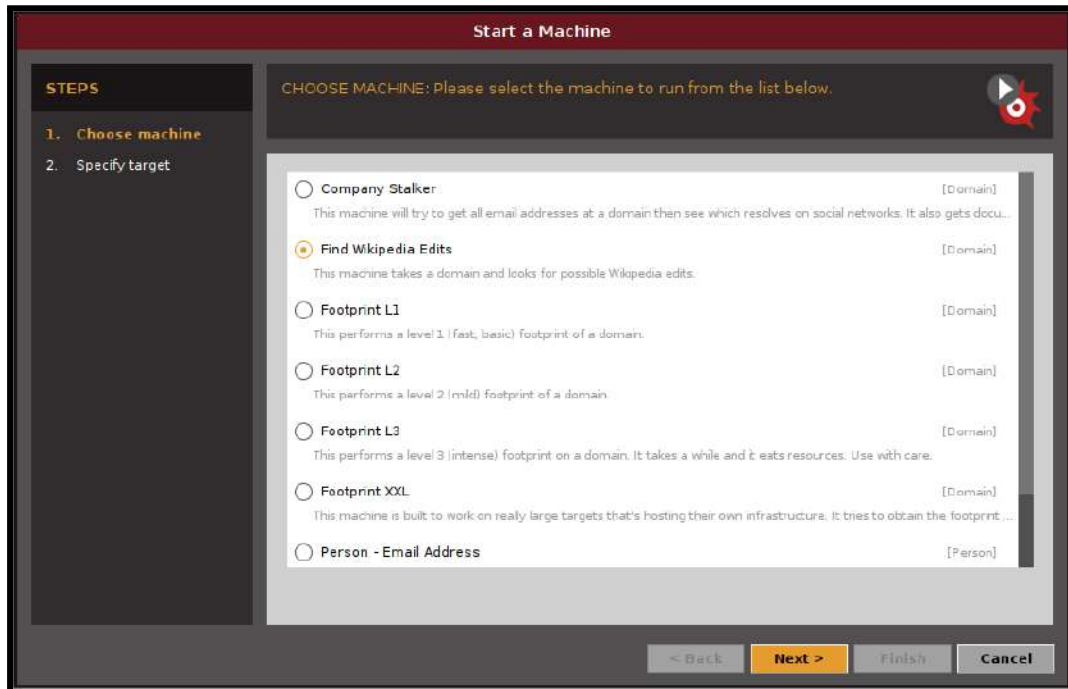


When we Search for Websites Mentioning Domain on www.github.com :

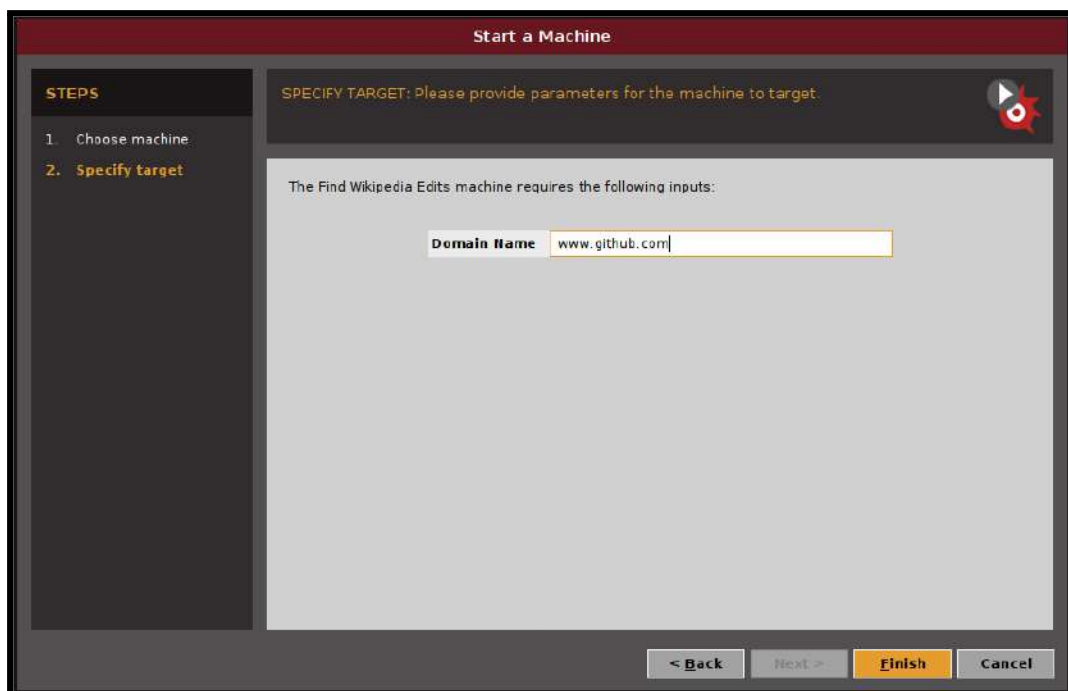


Steps to Start a Machine for Information Gathering [Find Wikipedia Edits]:

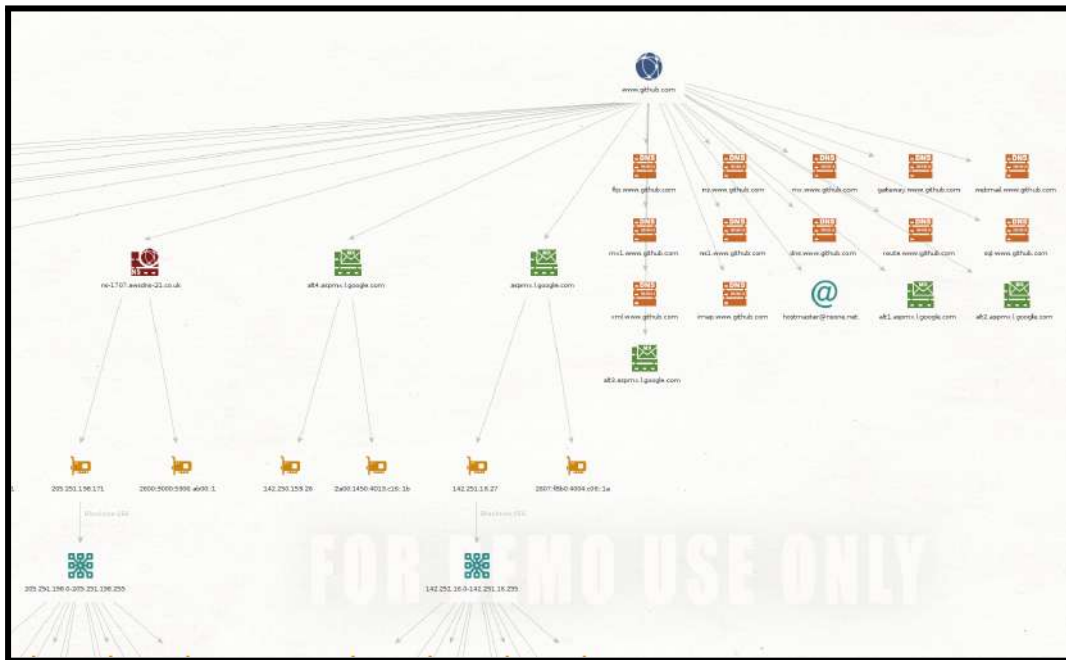
Step 1 : We will choose the Find Wikipedia Edits machine that we will use.



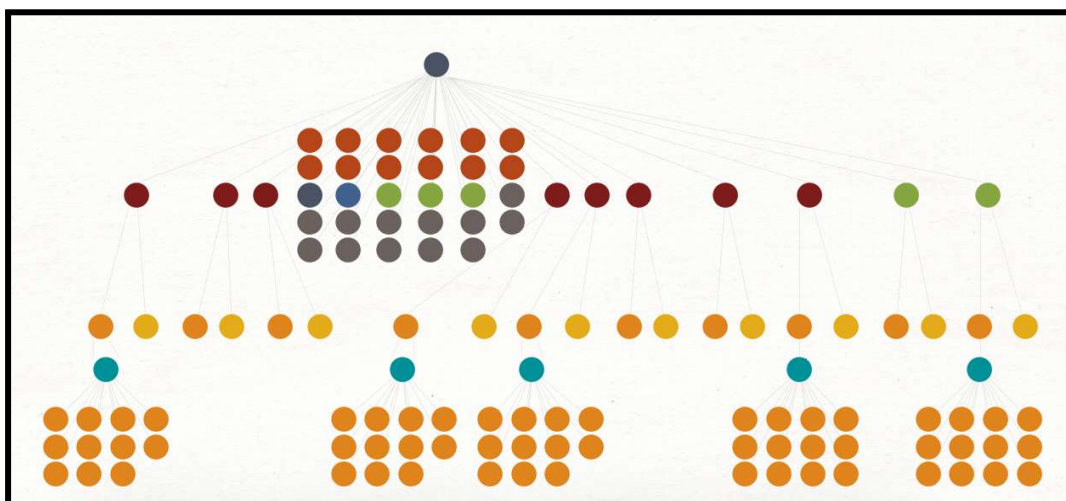
Step 2 : We will define our target domain name



Step 3 : We will get the following graph for the given Domain



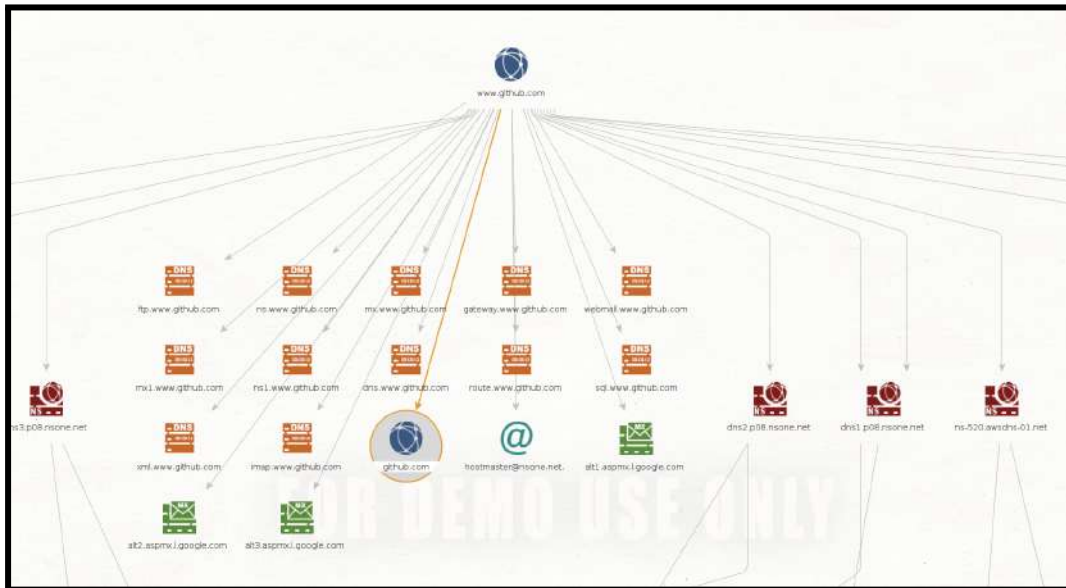
Graph :



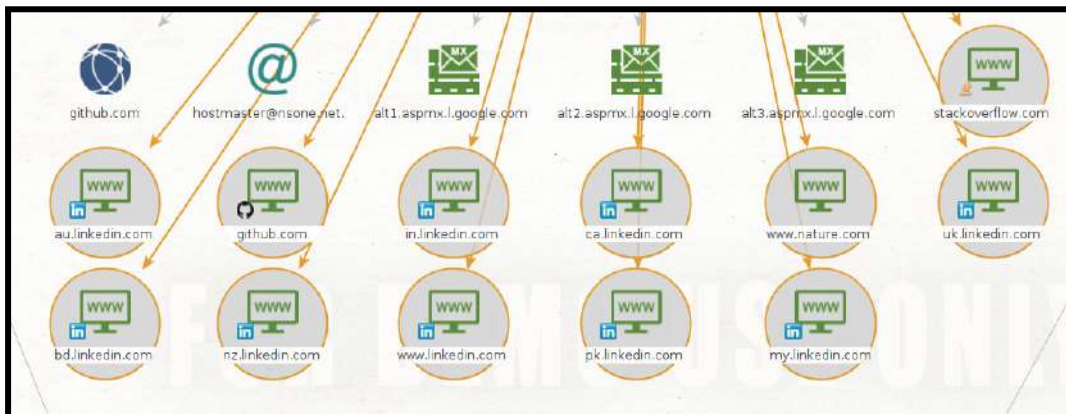
Different Node Representation :



When we Search for Domain :

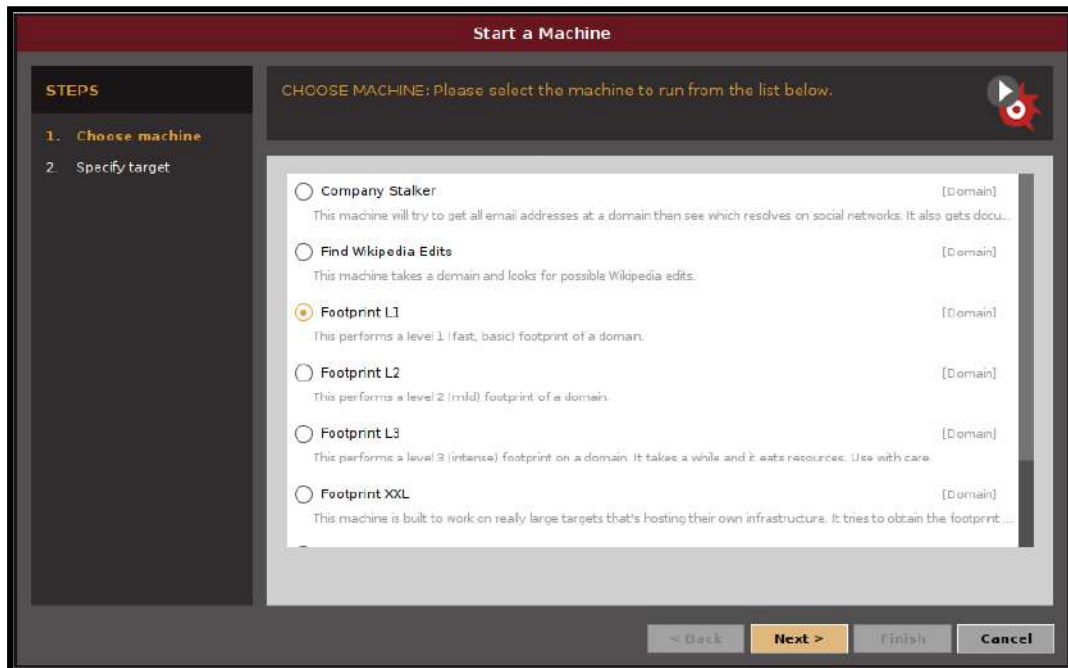


When we search for Websites for www.github.com :

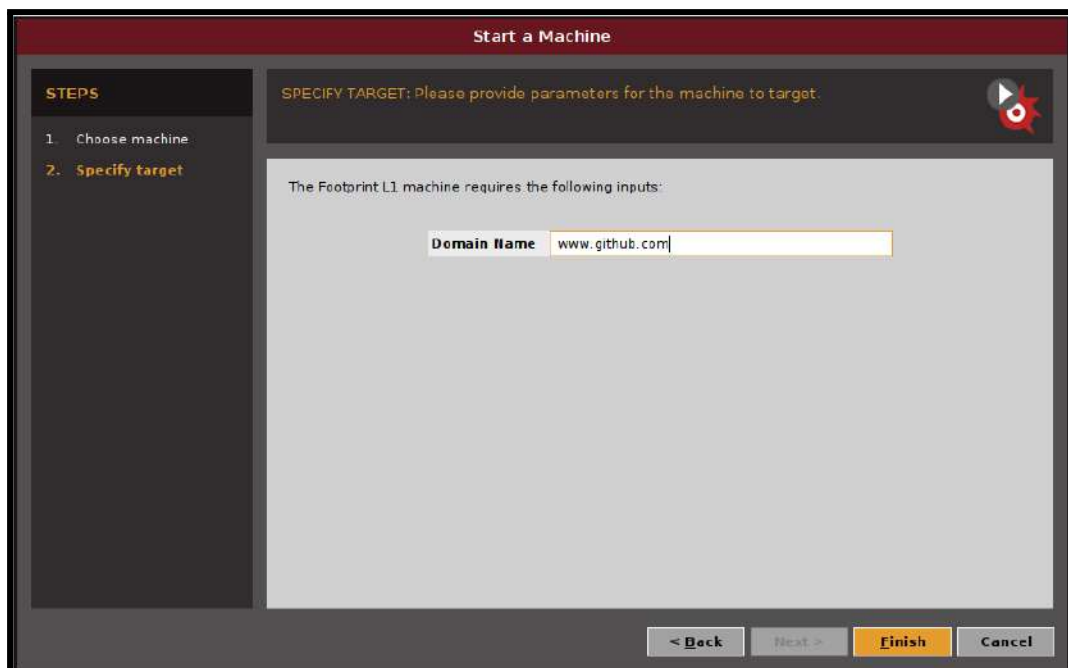


Steps to Start a Machine for Information Gathering [Footprint L1]:

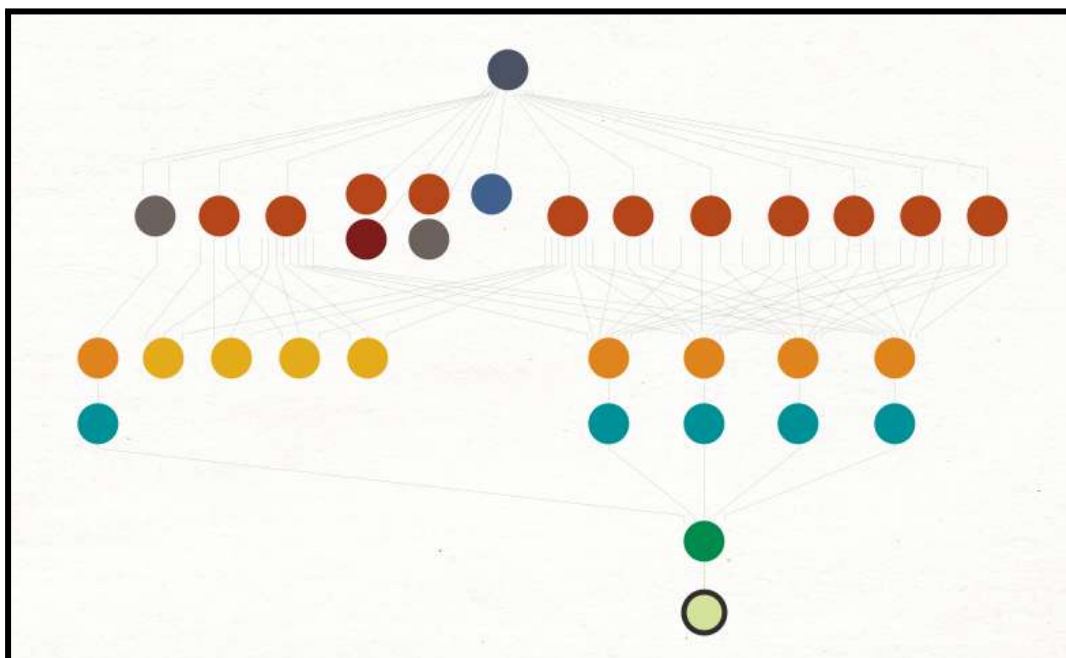
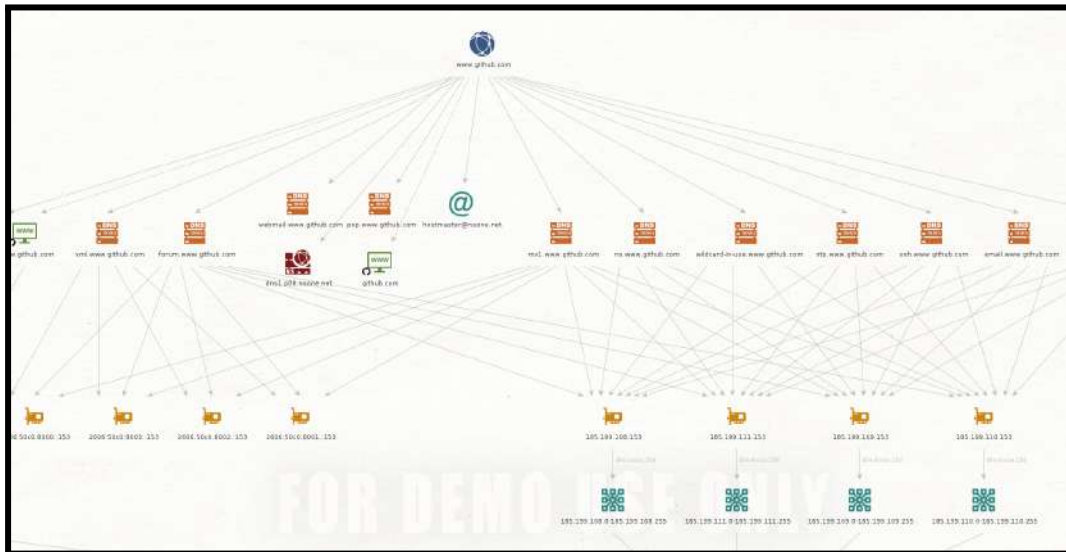
Step 1 : We will choose the Footprint L1 machine that we will use.



Step 2 : We will define our target domain name



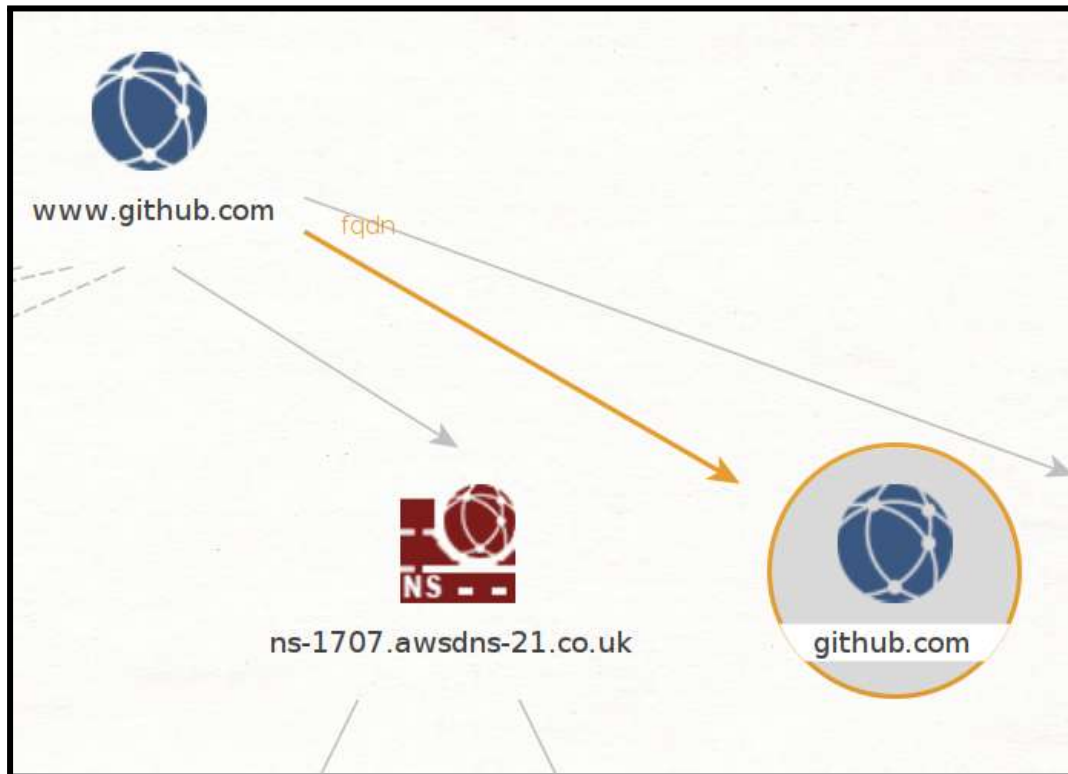
Step 3 : We will get the following graph for the given Domain



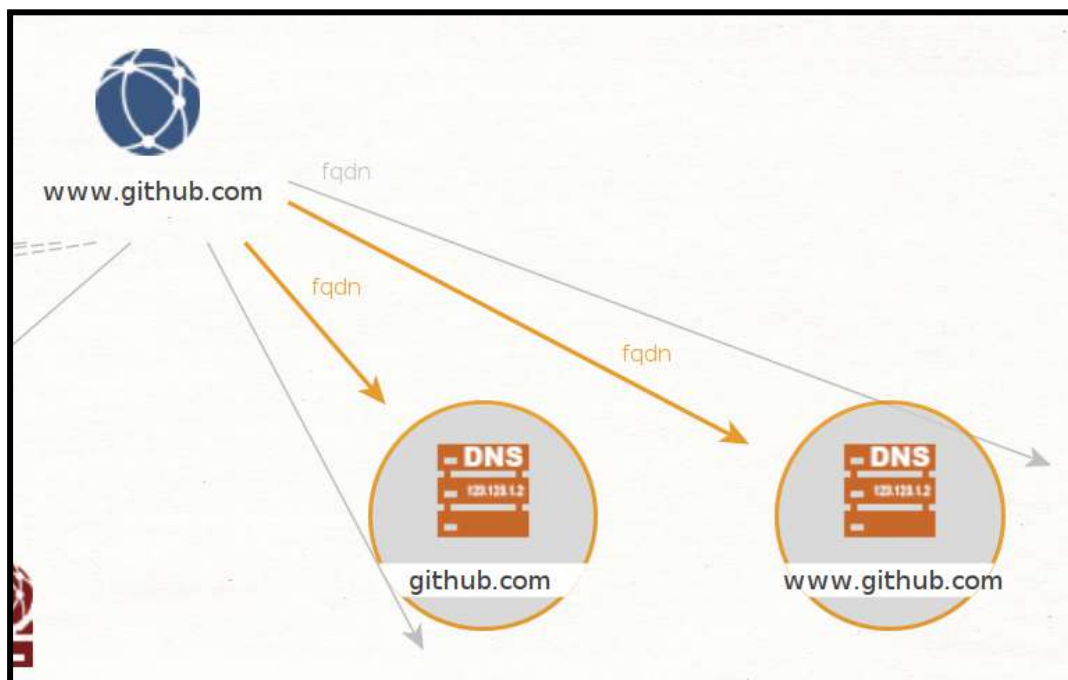
Different Node Representation :



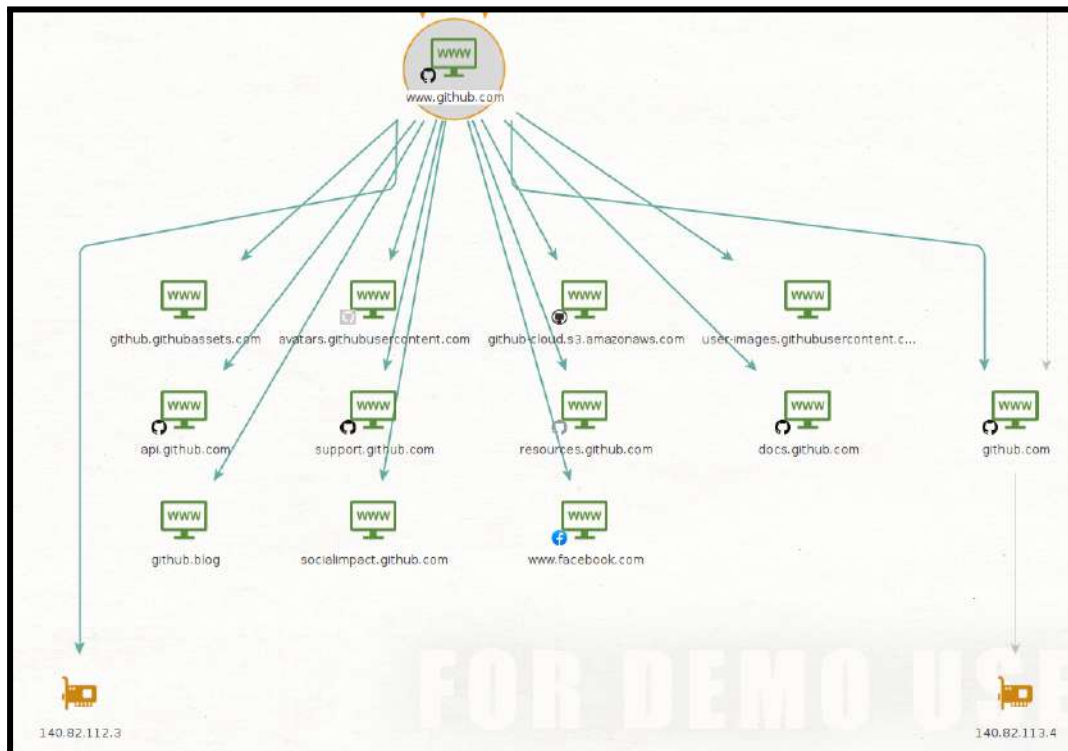
When search for Domains of www.github.com :



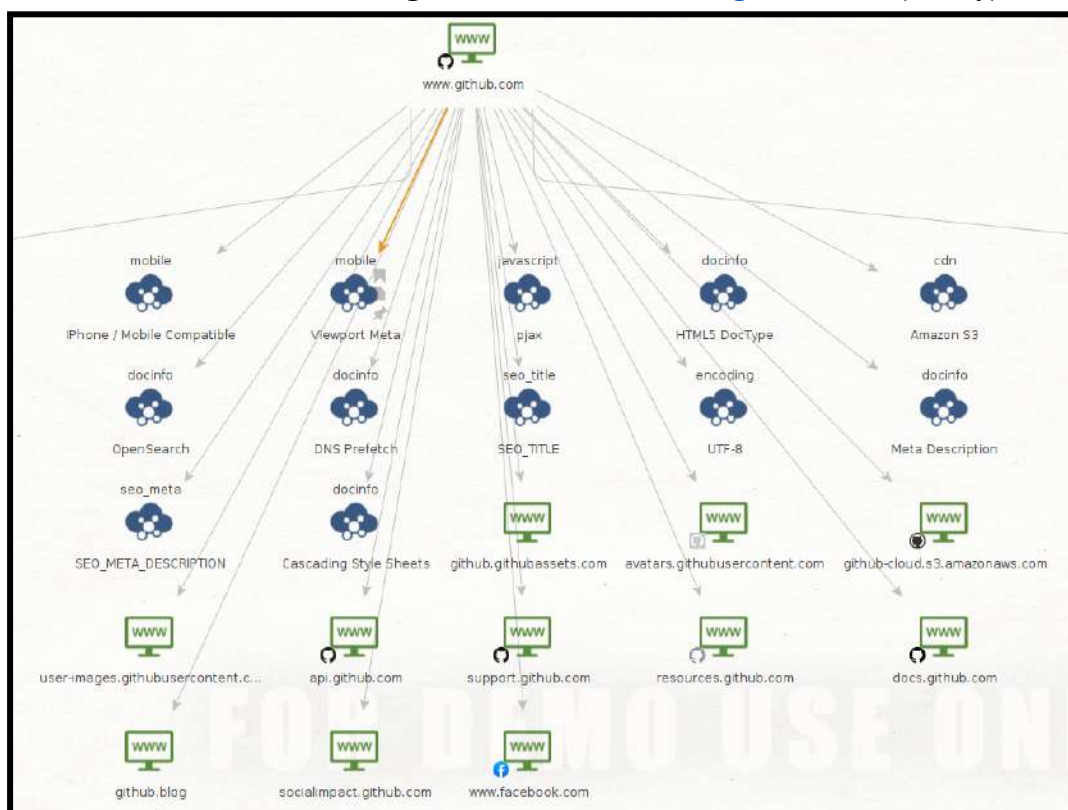
When we Search for DNS Names :



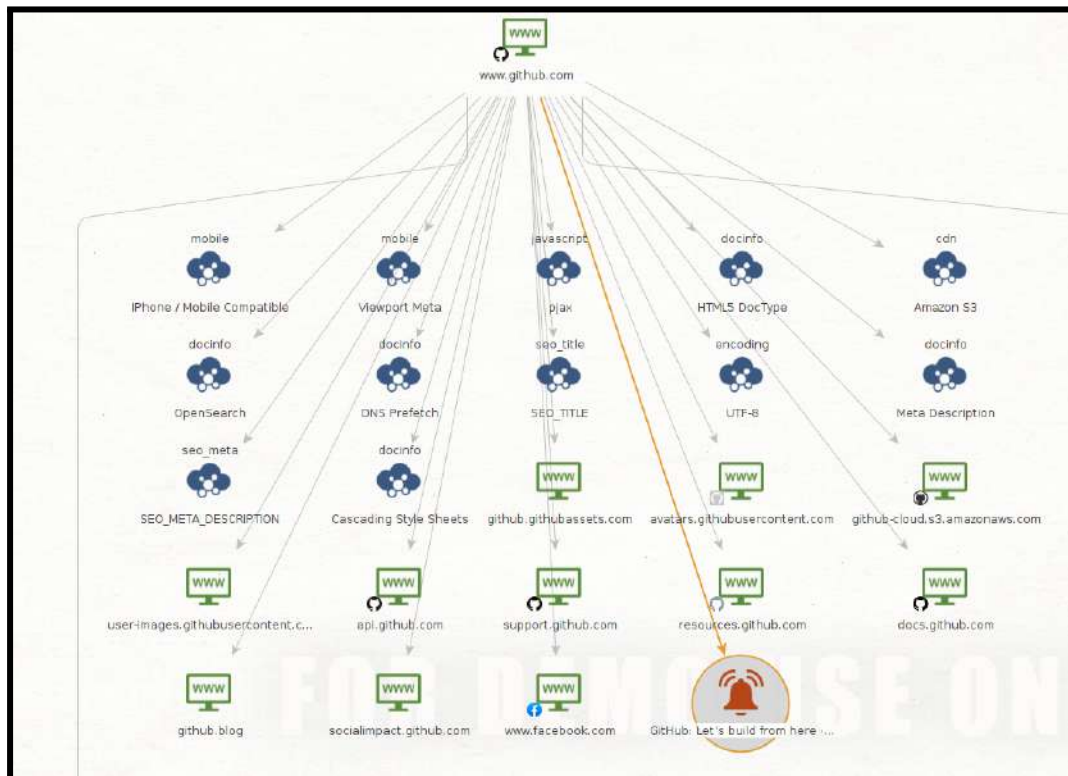
When we Search for External links on www.github.com (Entity)



When we Search for Technologies Built With on www.github.com (Entity):

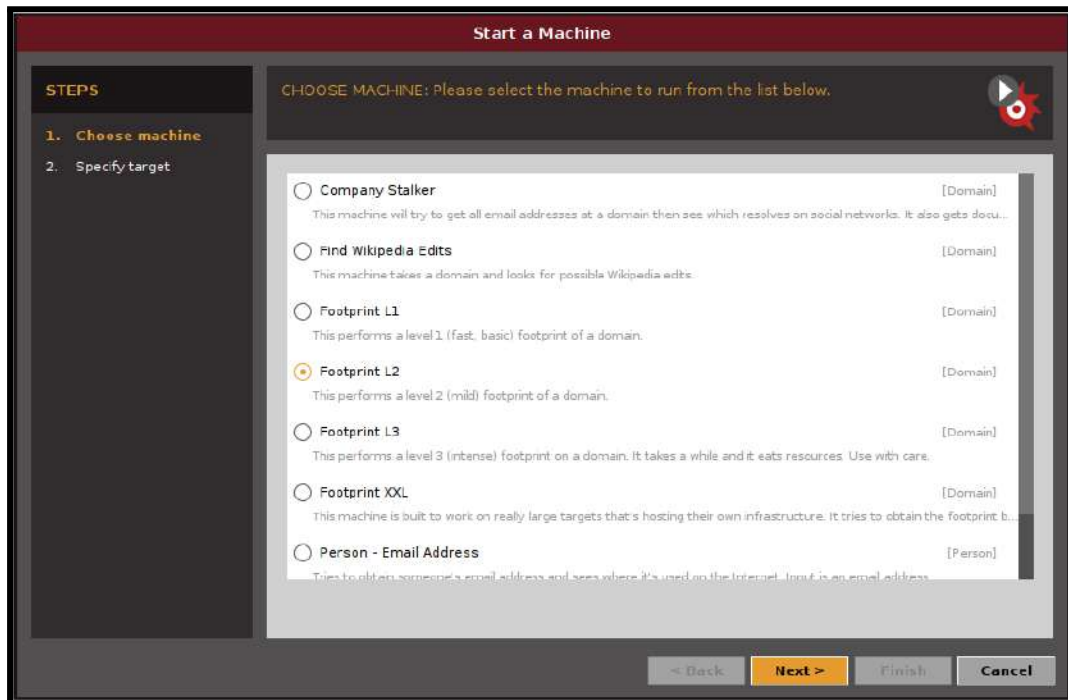


When we Search for Website Title on www.github.com (Entity):

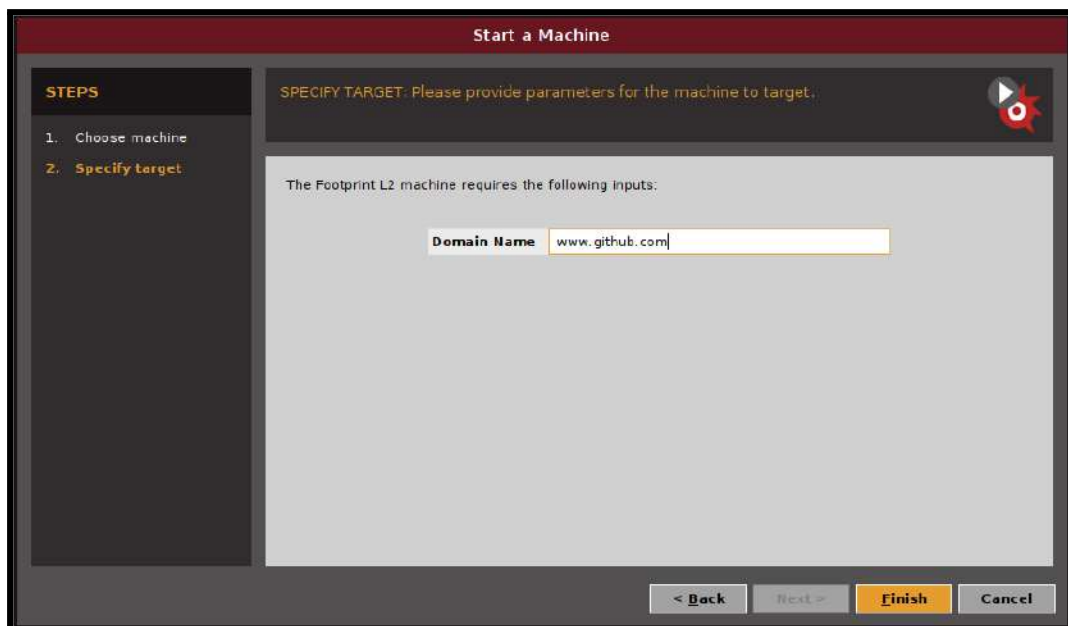


Steps to Start a Machine for Information Gathering [Footprint L2]:

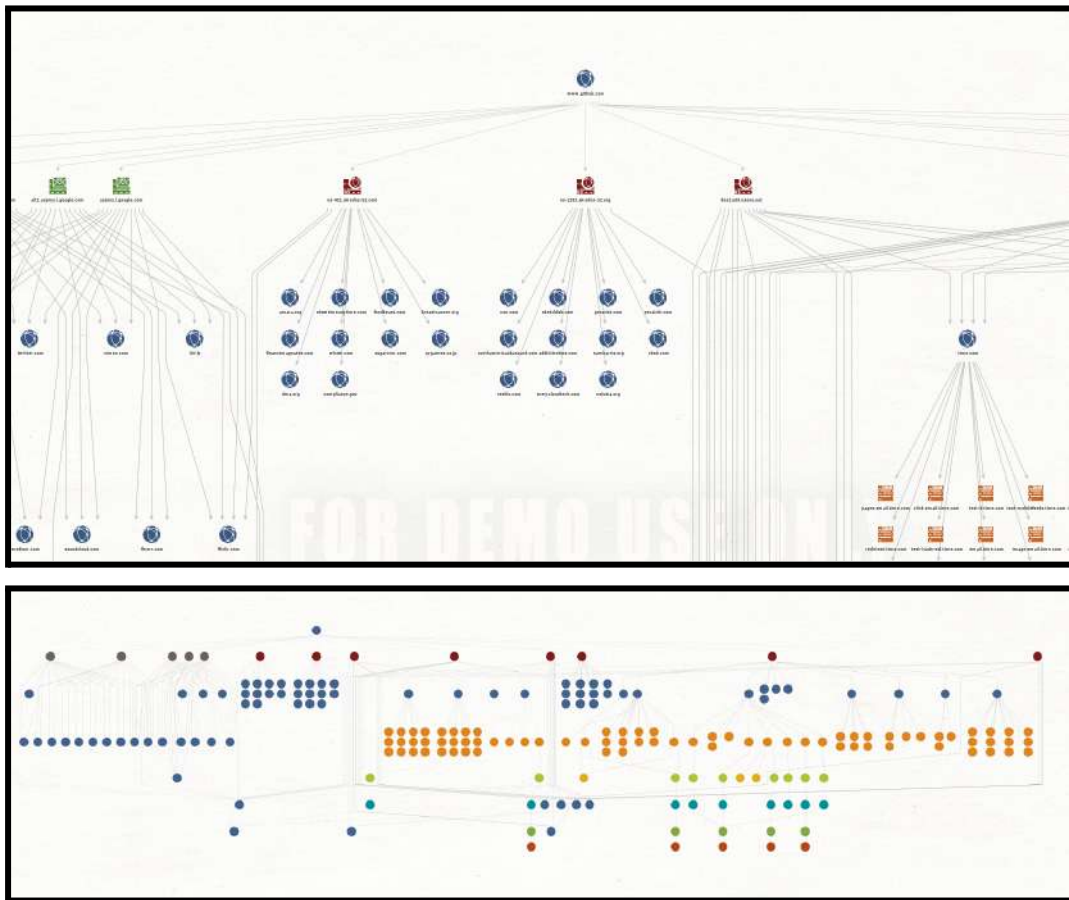
Step 1 : We will choose the Footprint L2 machine that we will use.



Step 2 : We will define our target domain name



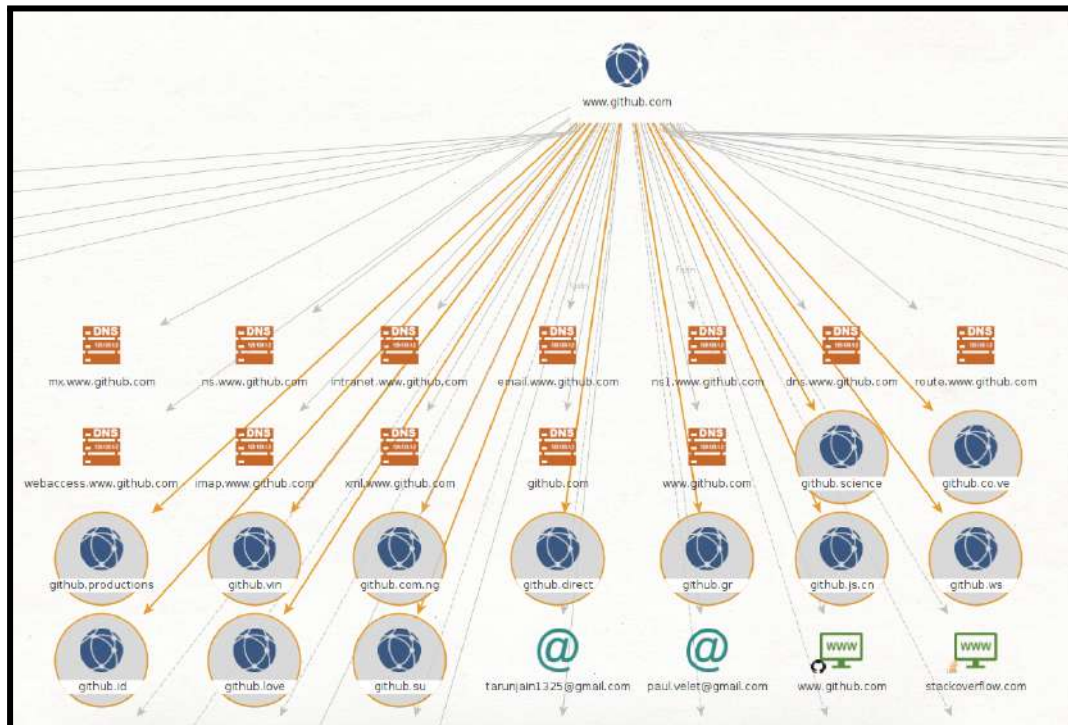
Step 3 : We will get the following graph for the given Domain



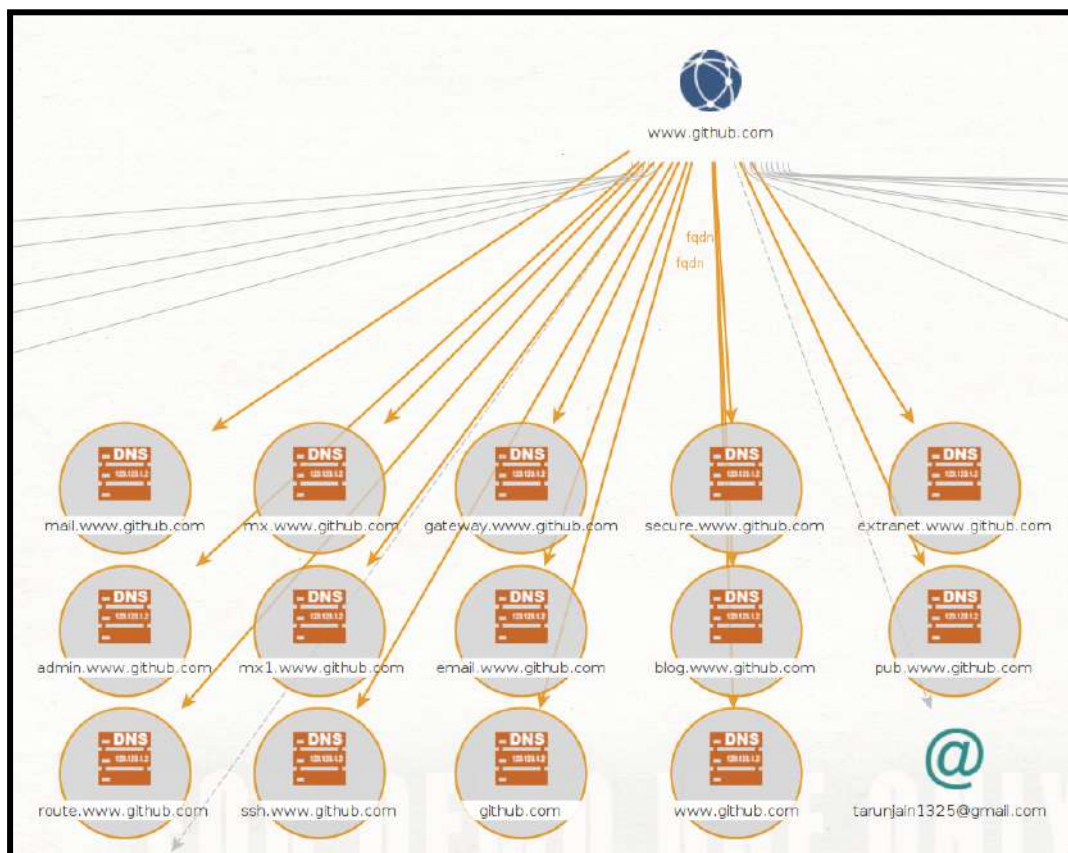
Different Node Representation :



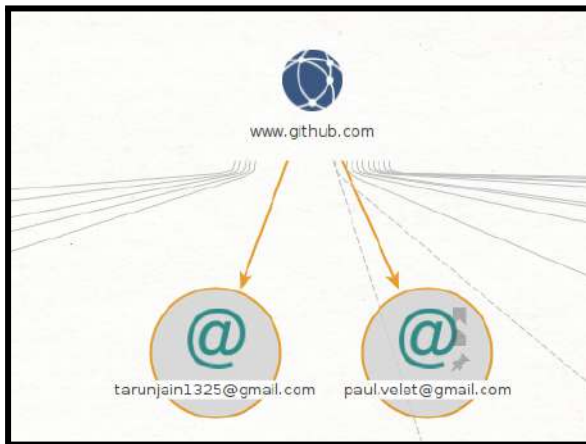
When search for Domains of www.github.com :



When we Search for DNS Names :



When we Search for Email Ids in www.github.com :



When we Search for Websites using www.github.com :

