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

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

   Output :
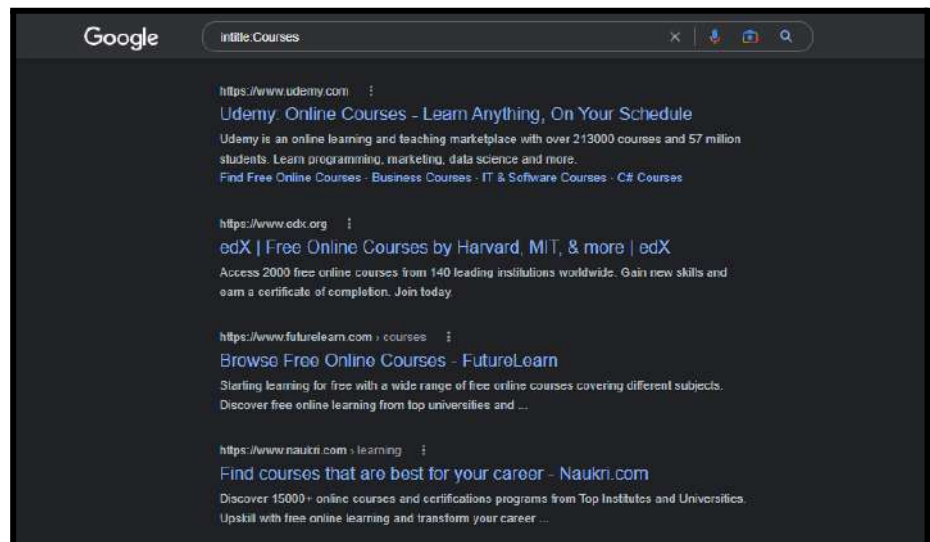
   ii. inurl

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

Output :
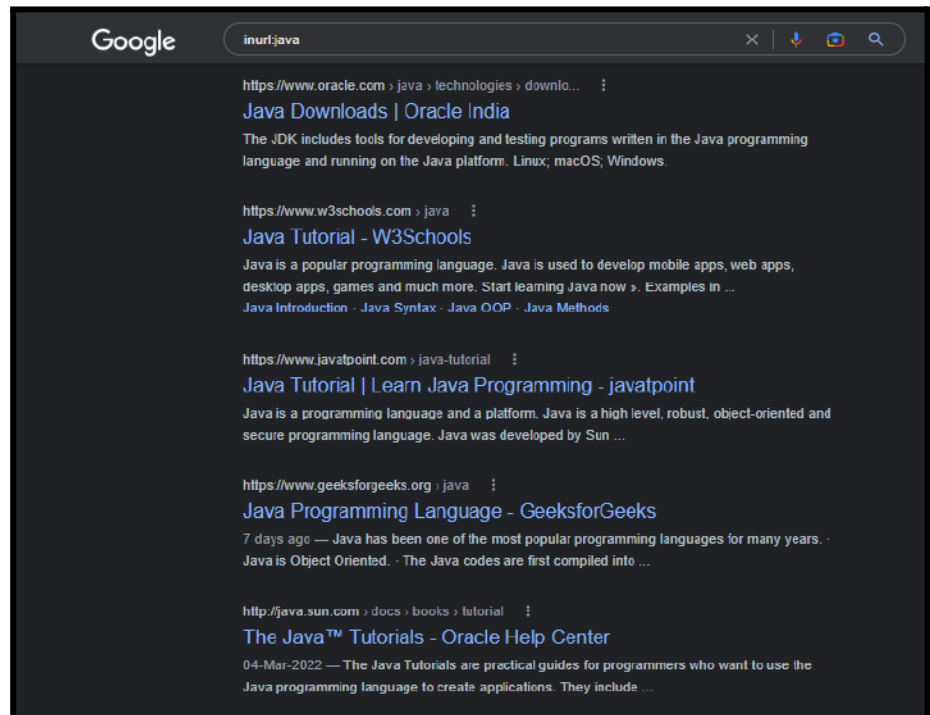
iii. filetype

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

    Output :
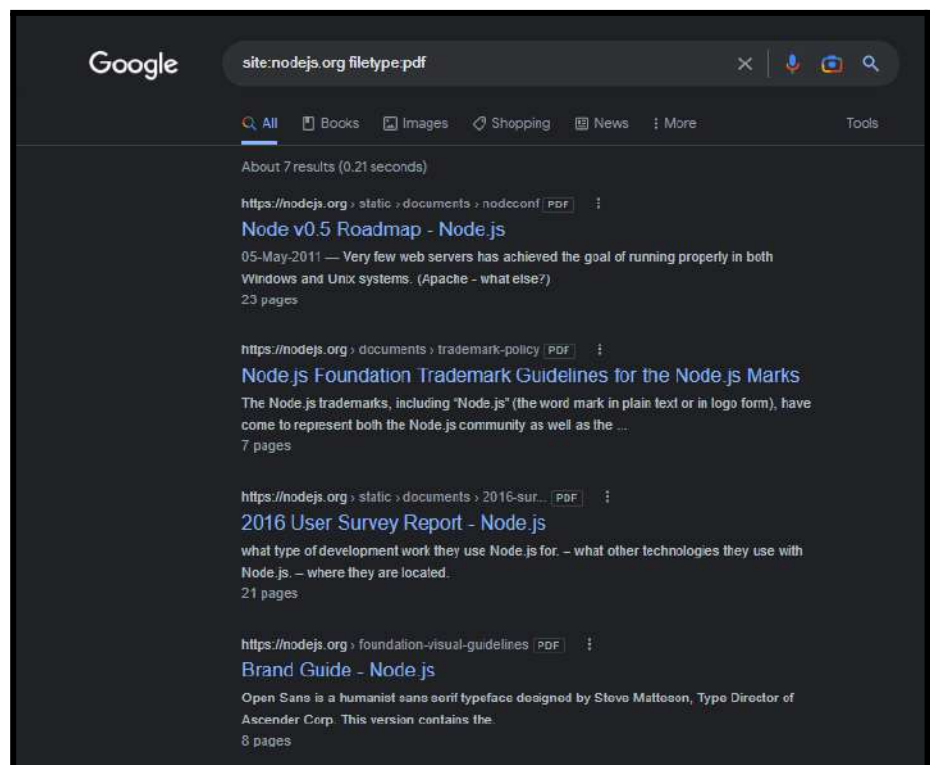
iv. ext

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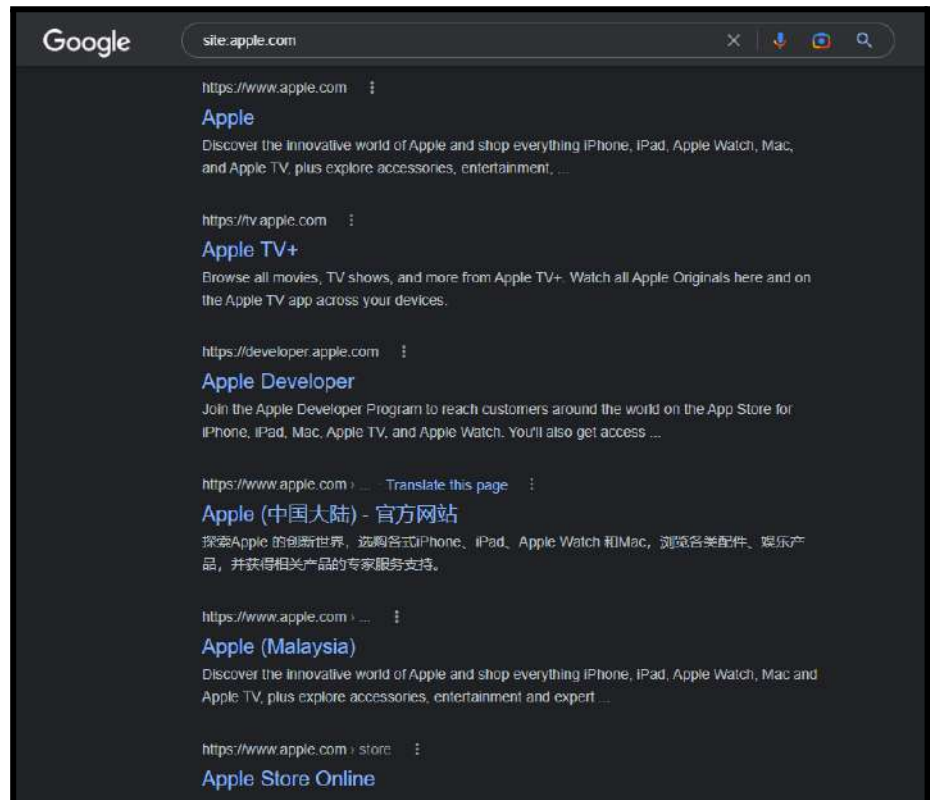
Output :
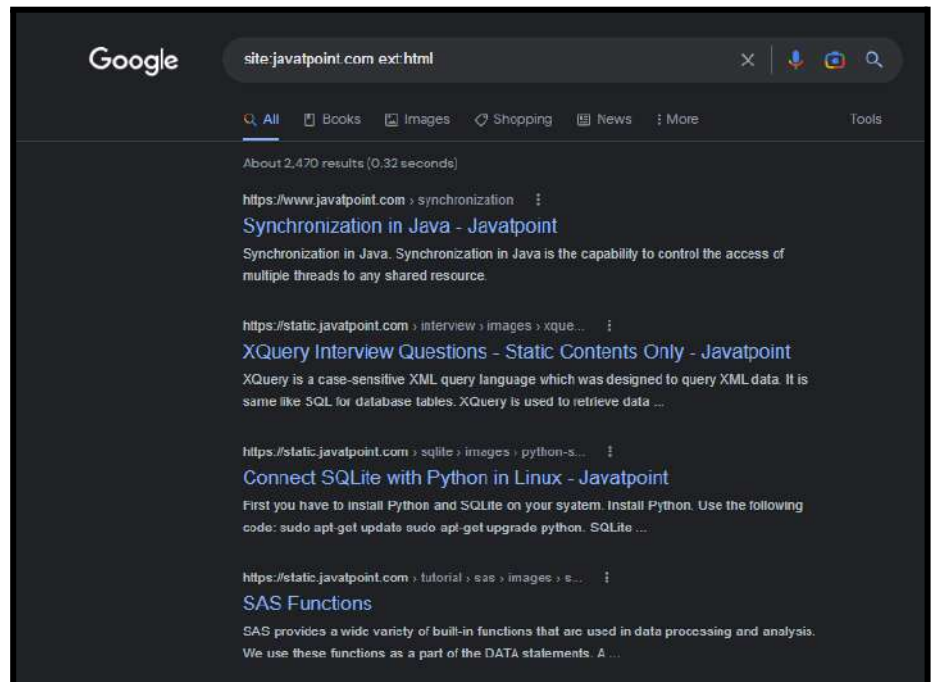
v. intext

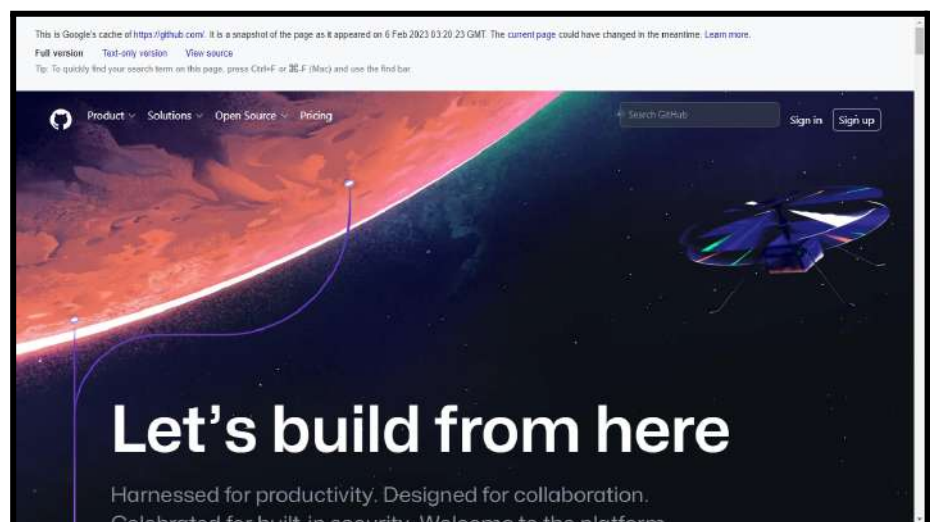**Descrpition :** This operator will find pages containing a certain word (or words) somewhere in the content.

Output :
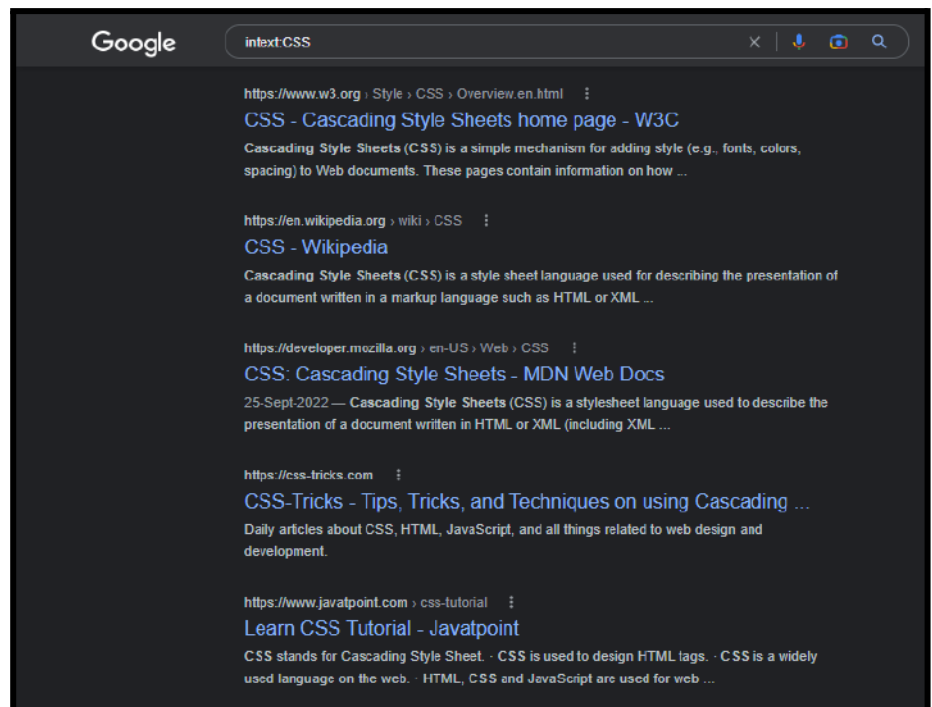
vi. site

Descrpition : This operator will give results of the specific website only.

Output :

vii. cache

Descrpition : This operator will returns the most recent cached version of a web page

Output :

viii. *

Descrpition : This is a wildcard and will match any word or phrase
Output :
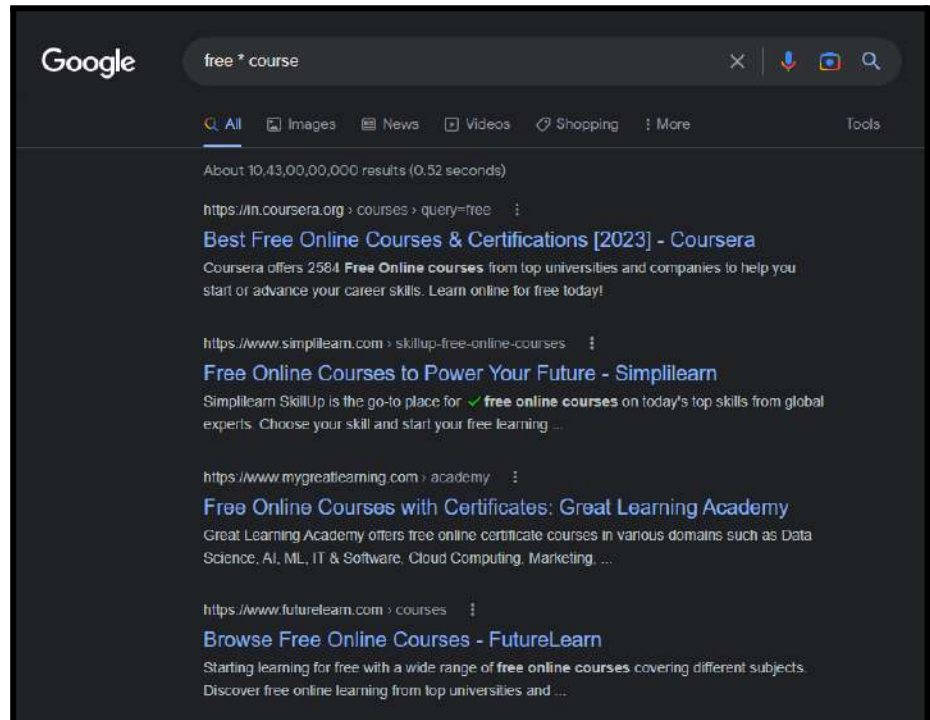
B. Perform any five dorks for the following categories :
   i. Files Containing Usernames

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

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

Output :

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

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 :

Google   intext:"index of" "phpinfo"

Q All   ⊘ Shopping   Images   News   ▶ Videos   ⋮ More   Tools

About 4,81,000 results (0.29 seconds)

datasistemasweb.com
https://plataformas.datasistemasweb.com › phpinfo   ⋮

Index of /phpinfo

Index of /phpinfo ; [PARENTDIR], Parent Directory, -.

matari-ad.com
http://www.matari-ad.com › phpinfo   ⋮

Index of /phpinfo

Index of /phpinfo ; [PARENTDIR], Parent Directory, -.

103.87.16
http://103.87.16.50   ⋮

Index of /

Index of /. [ICO], Name · Last modified · Size · Description. [TXT], index2.html, 2018-01-24 10:32, 11K. [ ], **phpinfo**.php, 2018-04-17 22:53, 23.

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.datasistemasweb.com Port 443

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

ii. Files Containing Usernames

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

Output :

Index of /usernames

Name	Last modified	Size	Description
Parent Directory		-	
BBCode.lastday.txt	2023-03-31 10:09	1.4K	
BBCode.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   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                             (Future IBIS development planned)
Scott Schlachter
955 East Arques Ave.
Sunnyvale, CA 94086-4533
(408) 522-4341
scotts@actel.com

Altera                            (Future IBIS development planned)
Gary Sugita
3 W. Plumeria
San Jose, CA 95134
(408) 894-7882
garys@altera.com


AMCC                              Misc. Models
Dick Spehn                        Bipolar and PECL
Tim Thompson                      BiCMOS
6195 Lusk Boulevard
San Diego, CA 92121-2793
(619) 535-6514
dicks@amcc.com
timt@amcc.com
```

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

Output :

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   intitle:"index of" "users.sql"

Q All   News   Images   Videos   Books   More   Tools

About 154 results (0.98 seconds)

csubak.edu
https://www.cs.csubak.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.csub.edu

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

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

Output :

iii. Various Online Devices

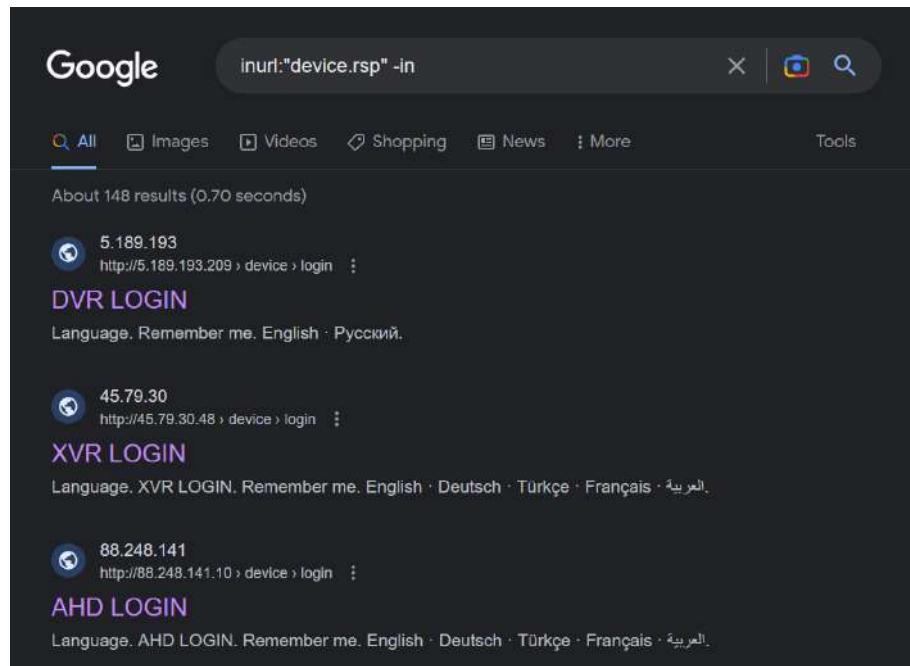**Dork 1 :** intitle:"NoVus IP camera" -com

Output :
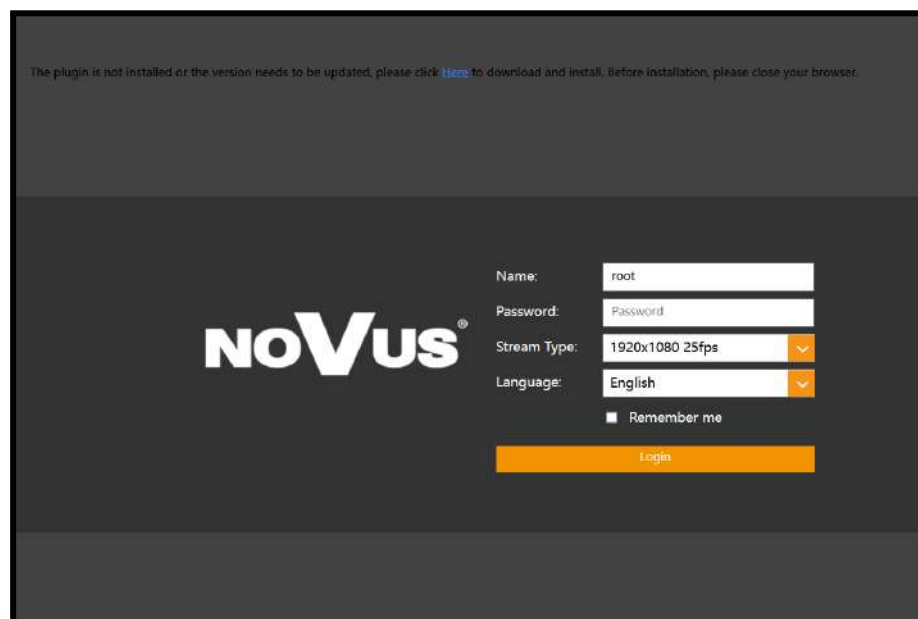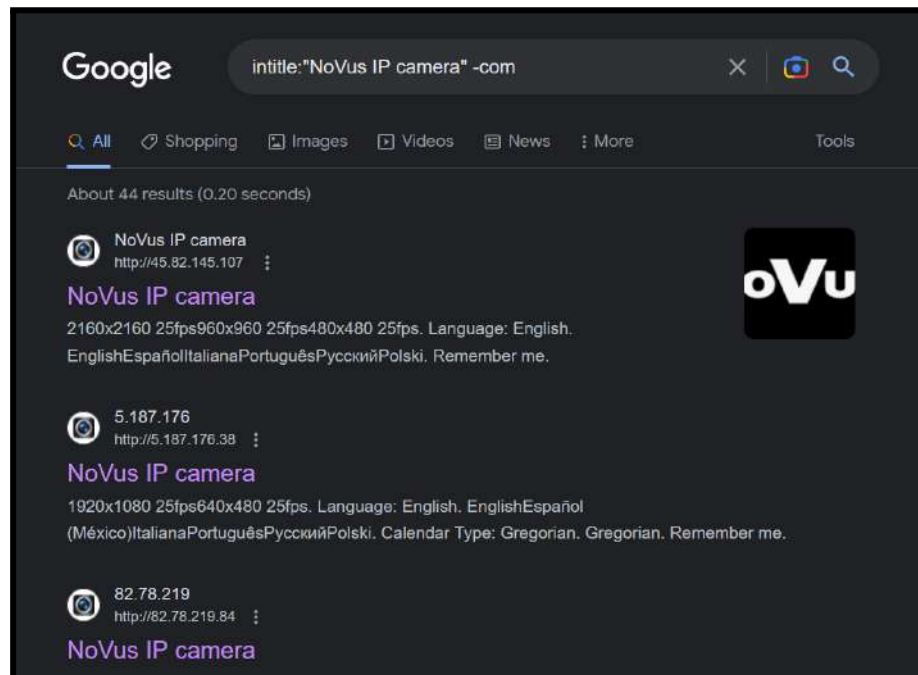
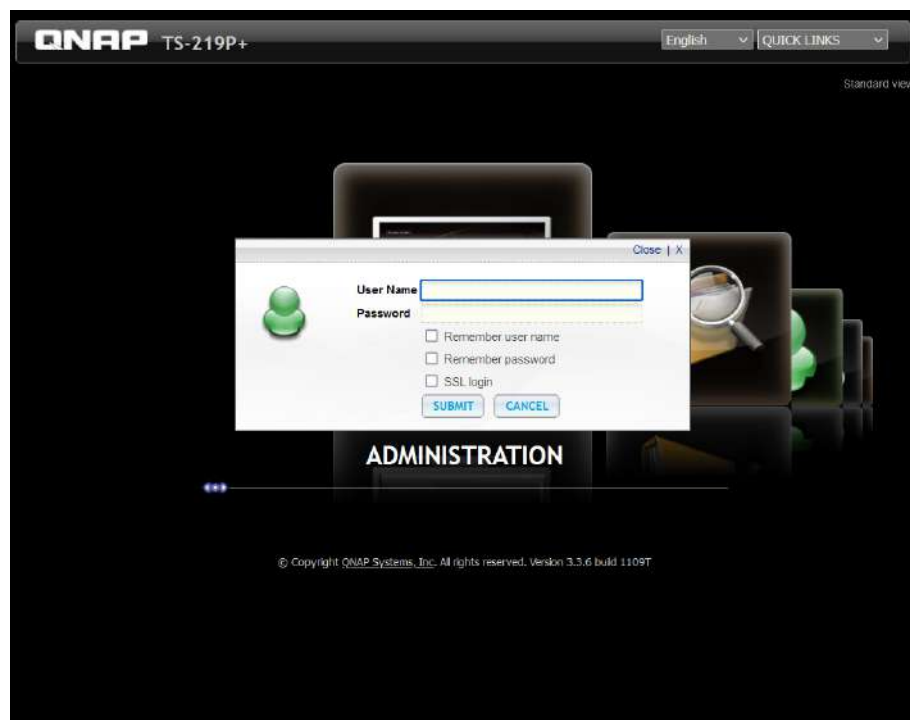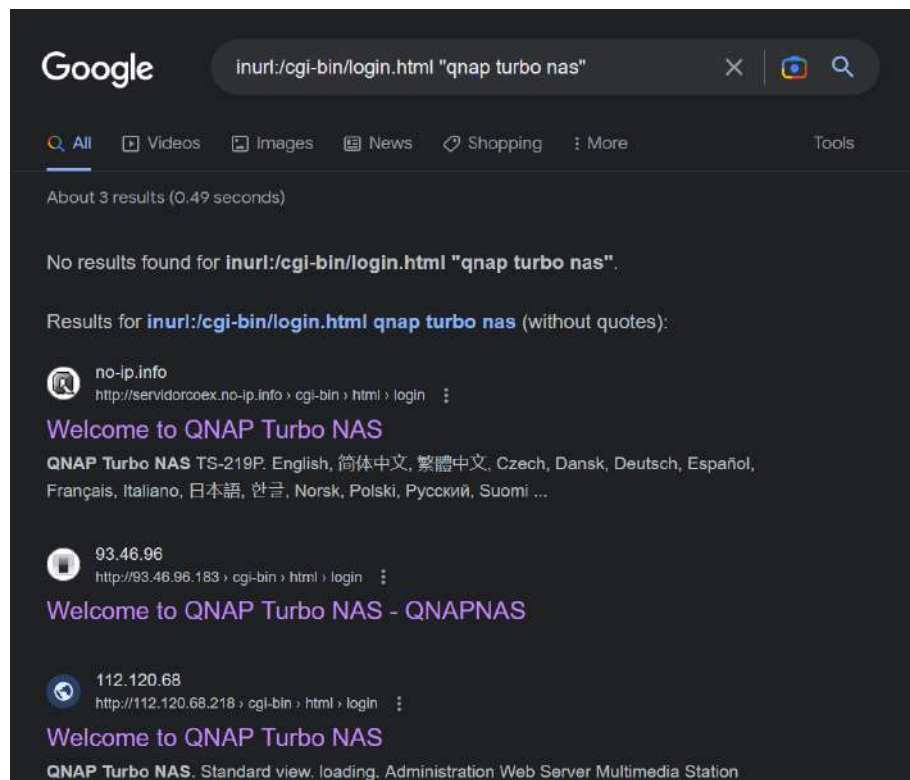**Dork 2 :** intitle:"Network Camera" inurl:main.cgi
Output :
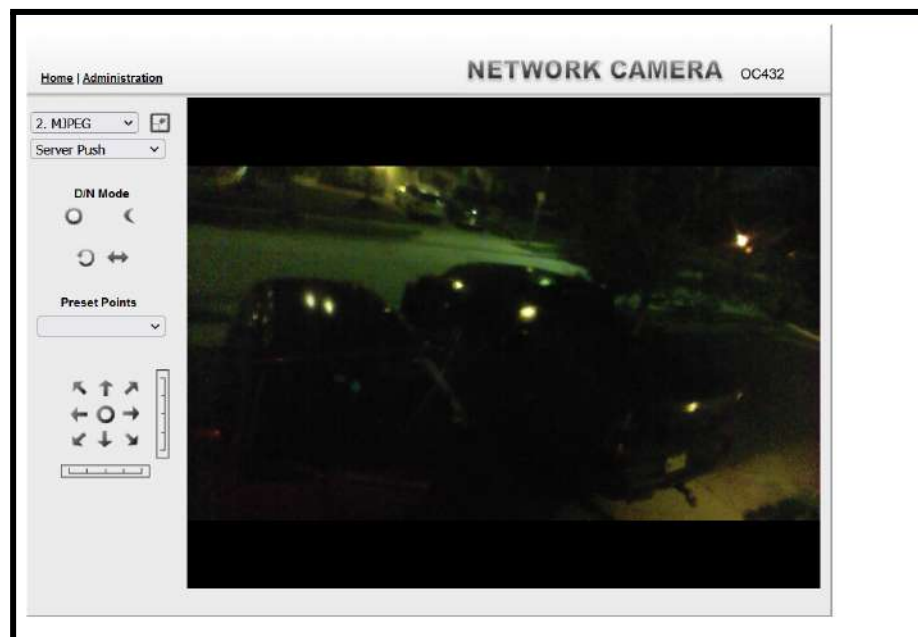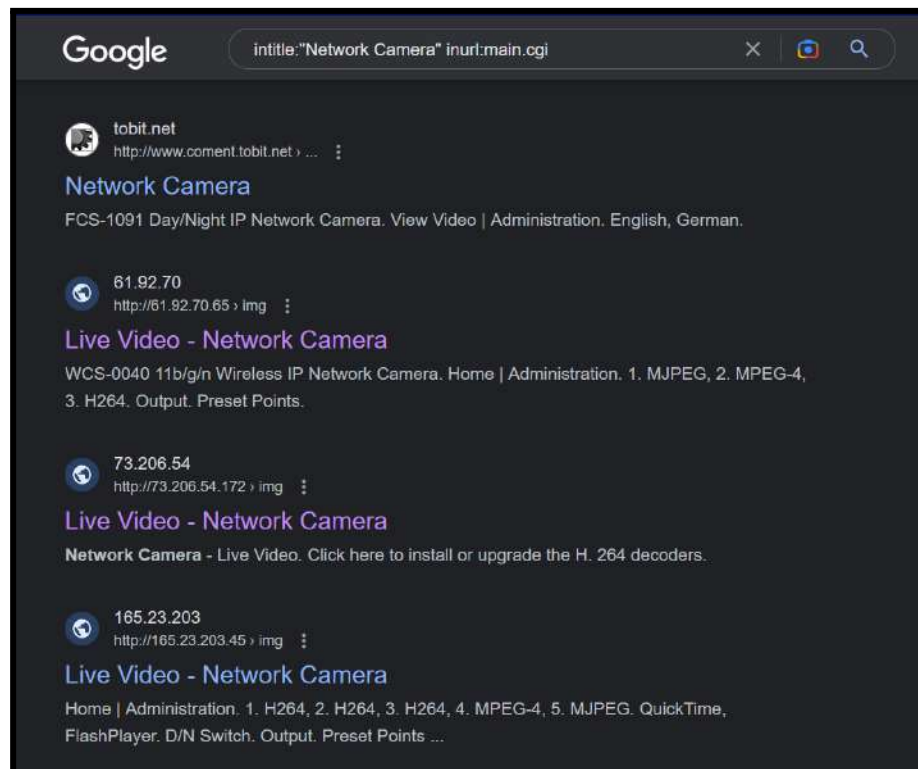
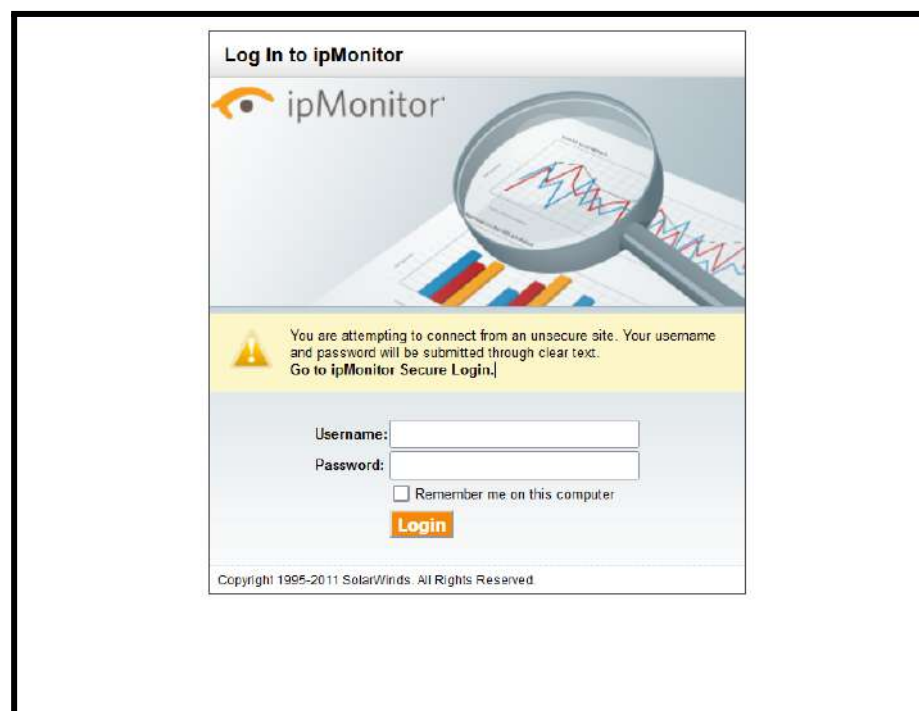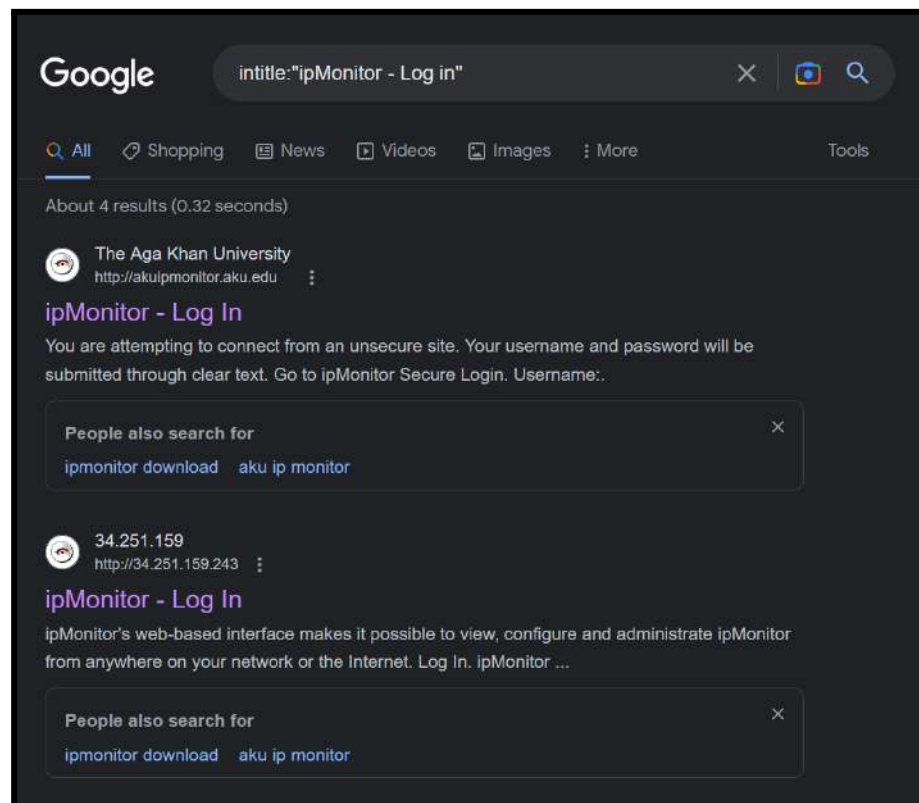**Dork 3 :** inurl:"device.rsp" -in
Output :

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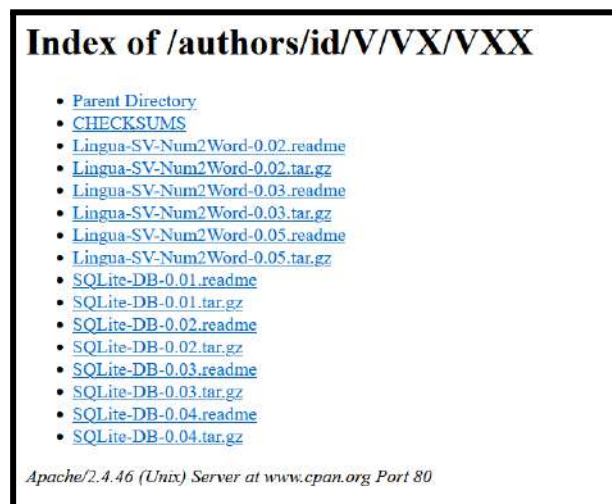**Output :**

Dork 5 : intitle:"ipMonitor - Log in"
Output :

iv. Sensitive Directories

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

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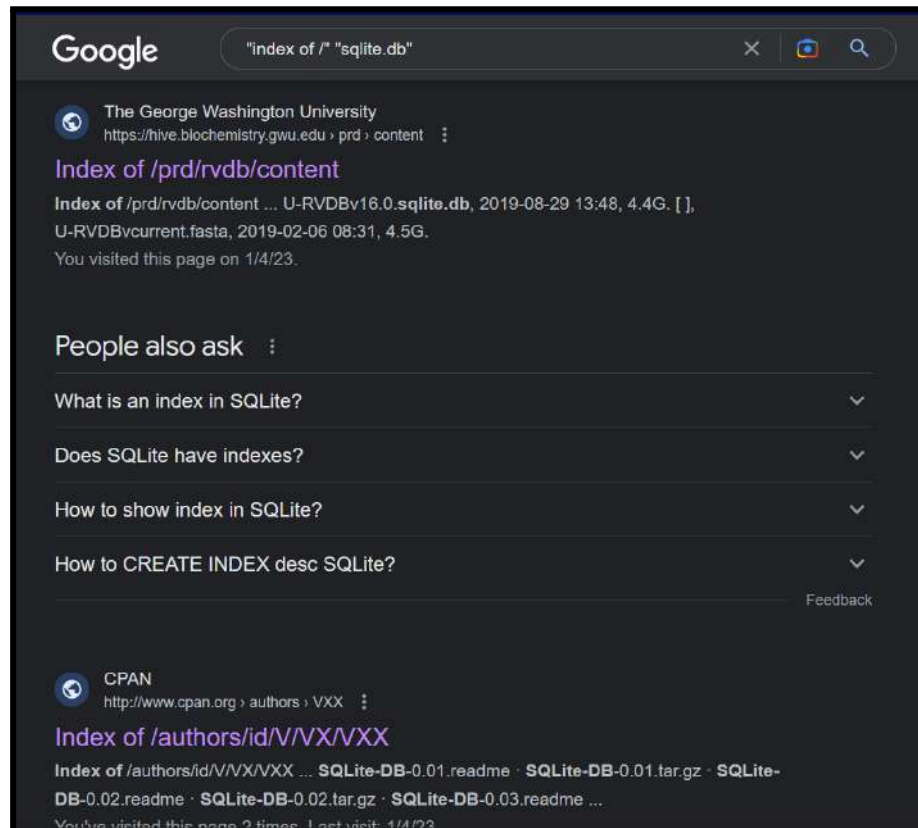
Dork 2 : intitle: "index of" "payment"

Output :

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 :

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

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

Output :

v. Vulnerable Files

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

Output :

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

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	-
awis.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
webocreationfeatured.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 :

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	-
js/	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 :

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

Output :

C. Write a dorks for the following:
  i. Log files for the login credentials
     Dork : allintext:password filetype:log
     Output :
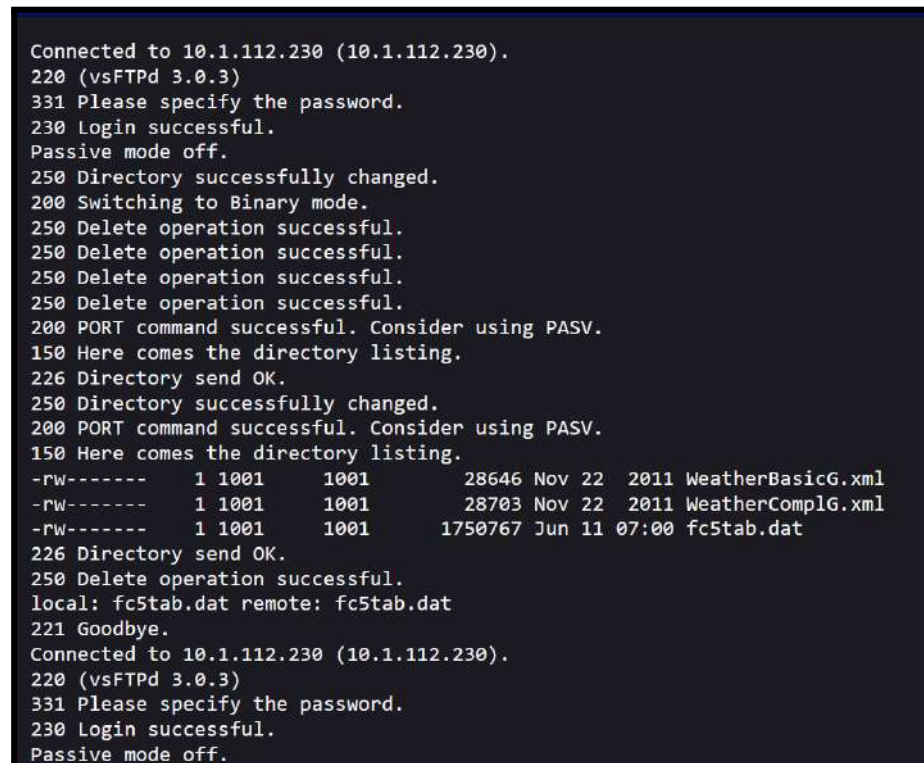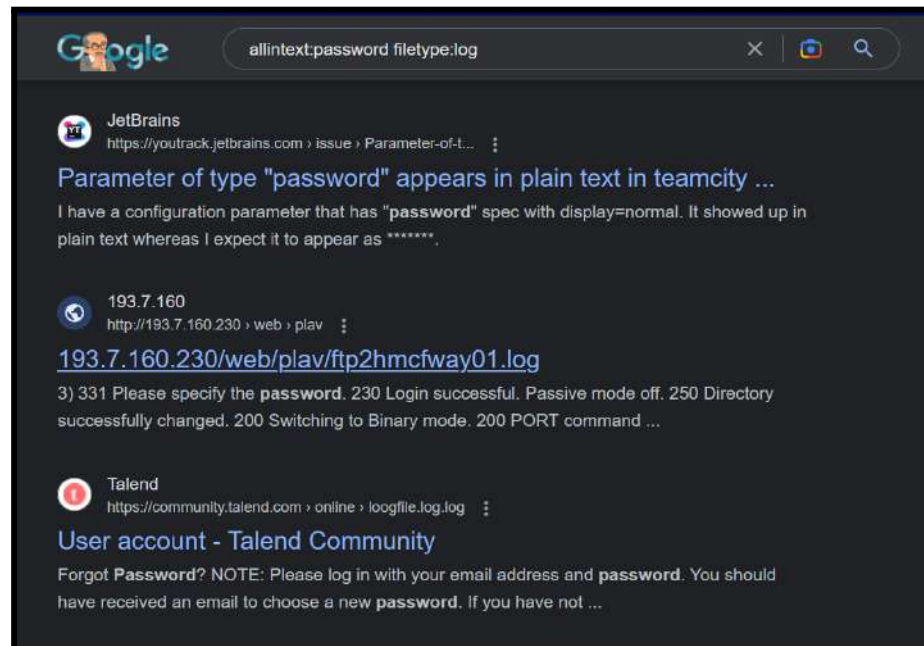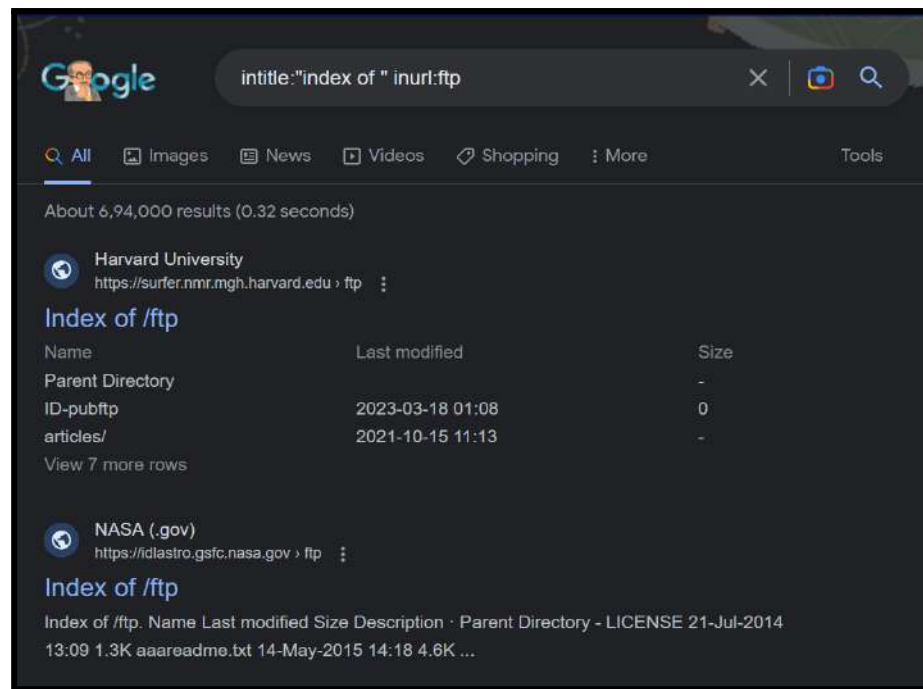

  ii. Open FTP servers
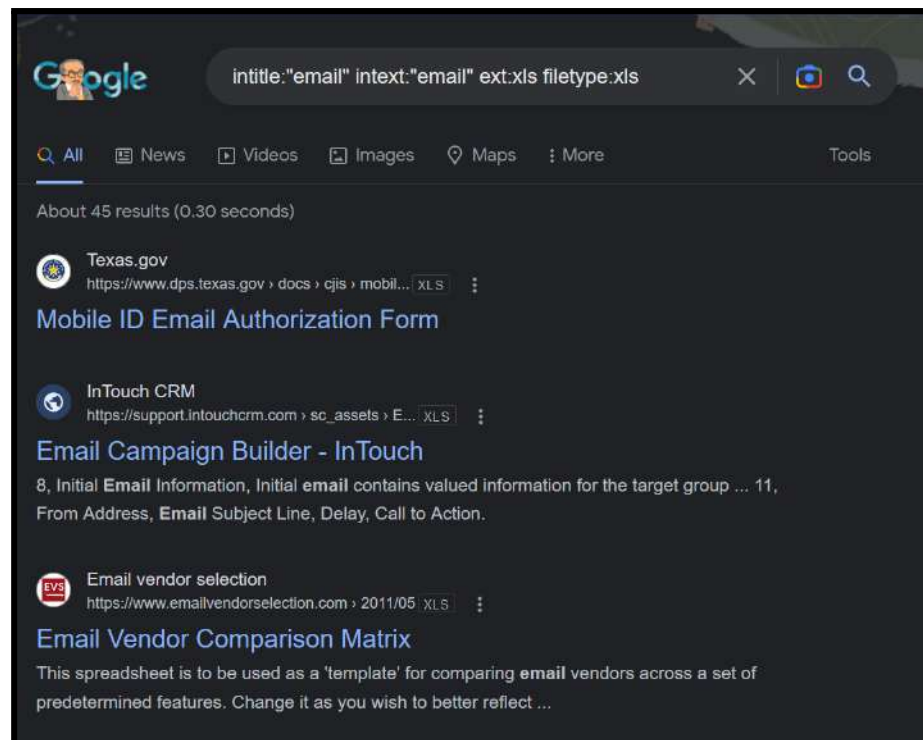   **Dork :** intitle:"index of " inurl:ftp
     Output :

iii. Fetch the excel files containing list if emails

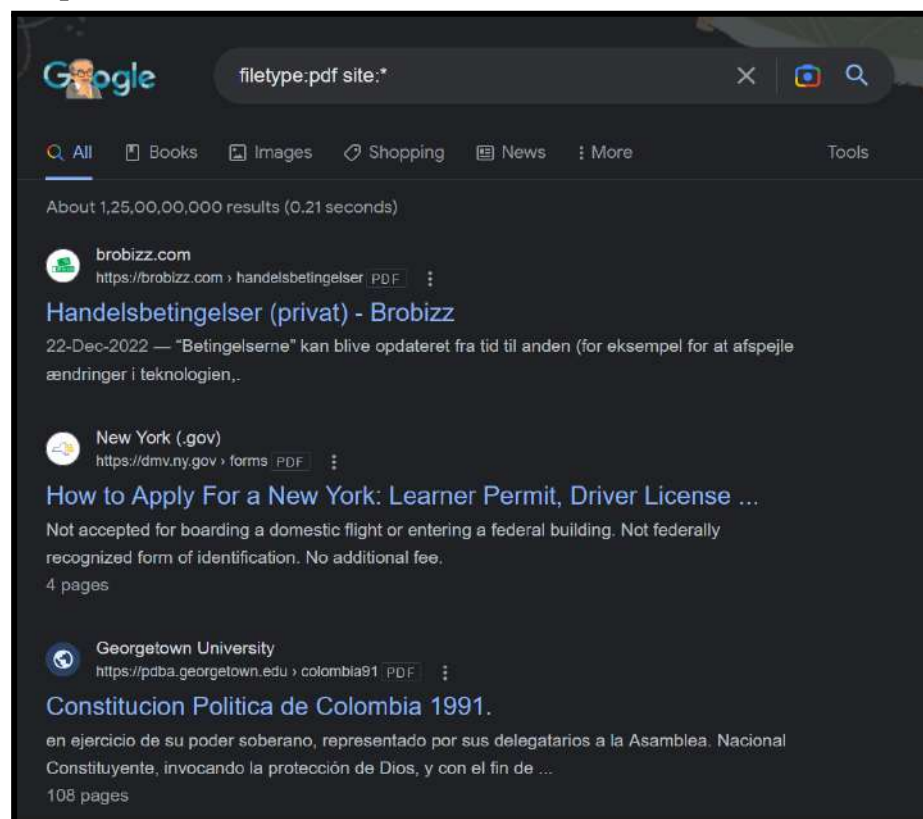**Dork :** intitle:"email" intext:"email" ext:xls filetype:xls

Output :

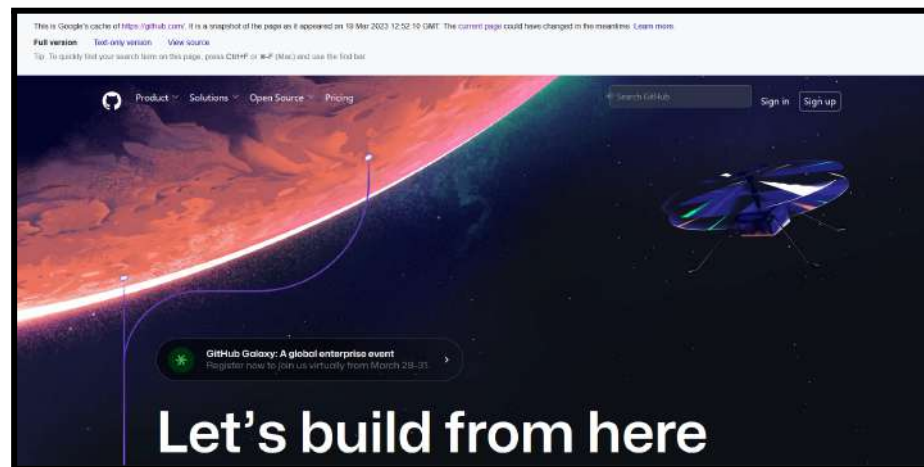iv. List only pdf files from the any website

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"**

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

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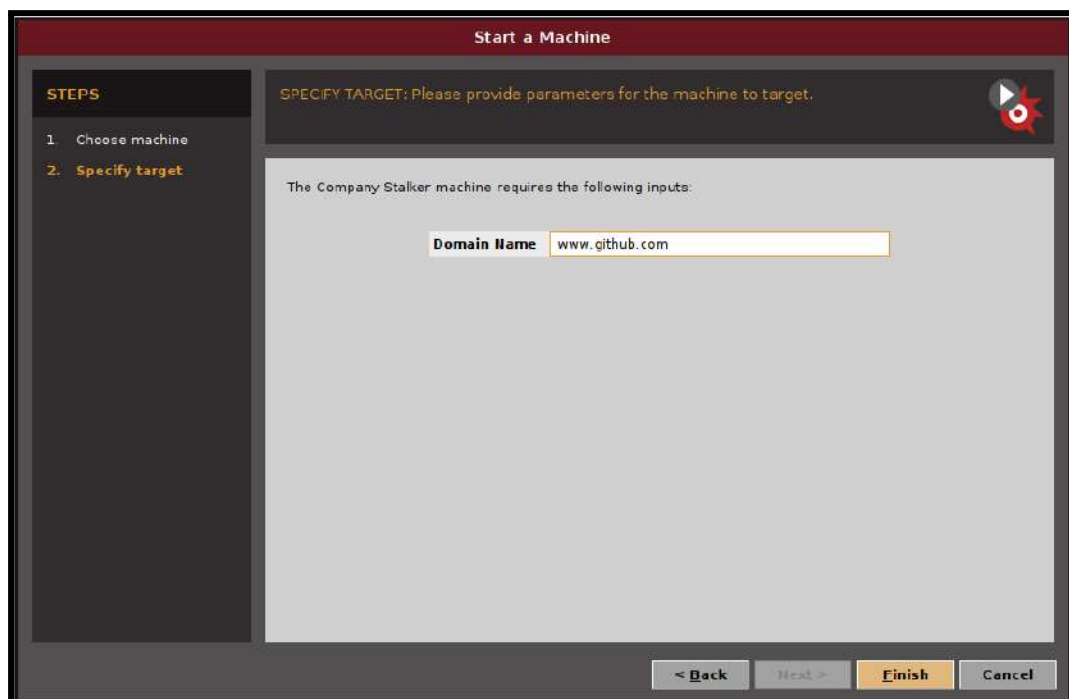
Footprint XXL :
This Machine is built to work on really large targets that are hosting their own infrastructure.

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

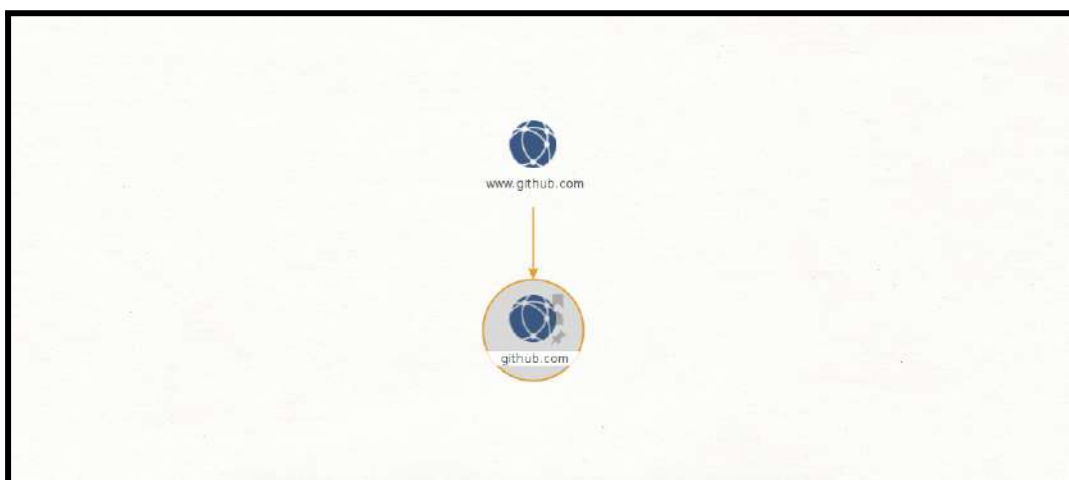**Step 1 :** We will choose the Company Stalker machine that we will use.
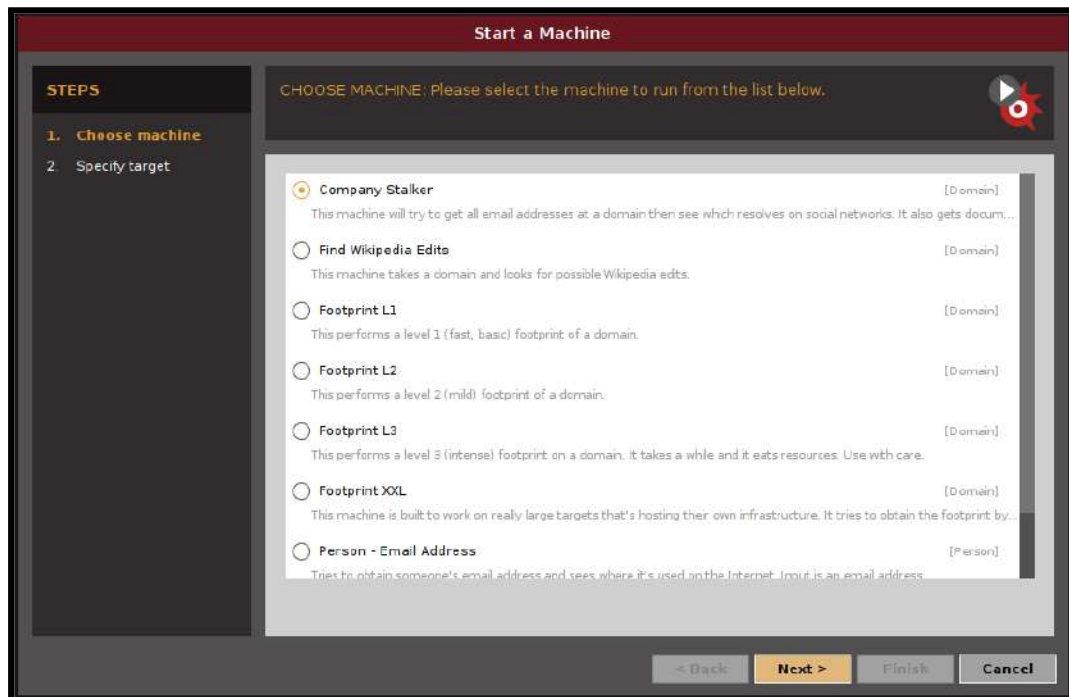
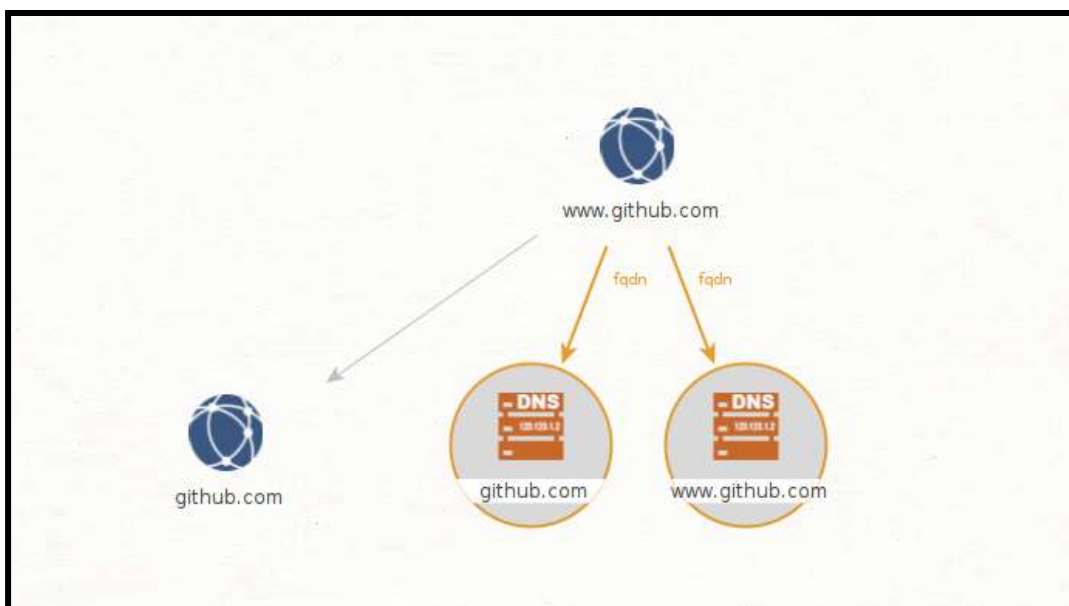**Step 2 :** We will define our target domain name

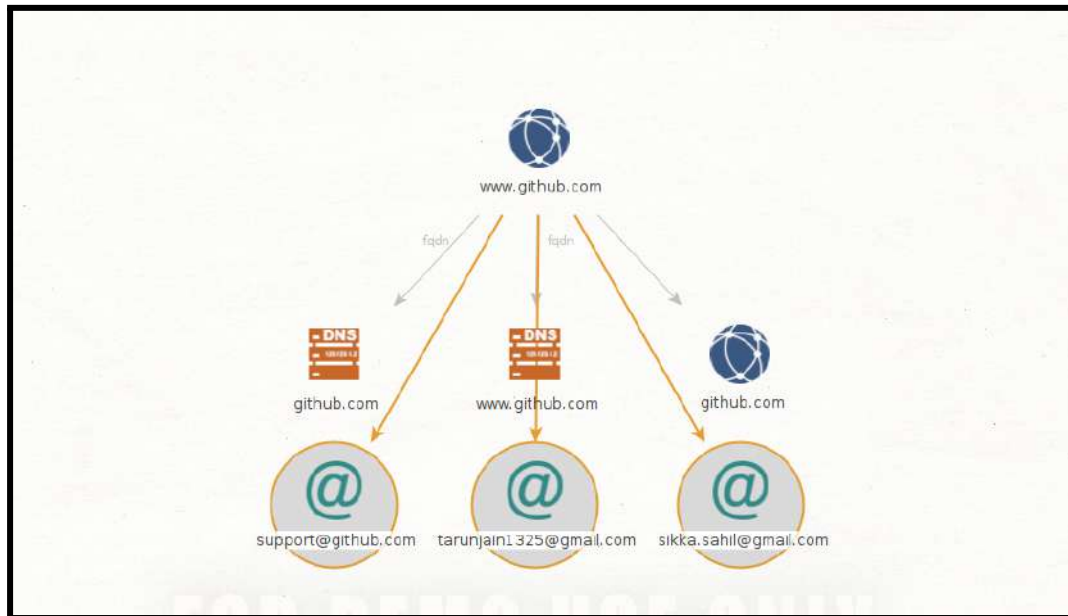**Step 3 :** We will get the following graph for the given Domain
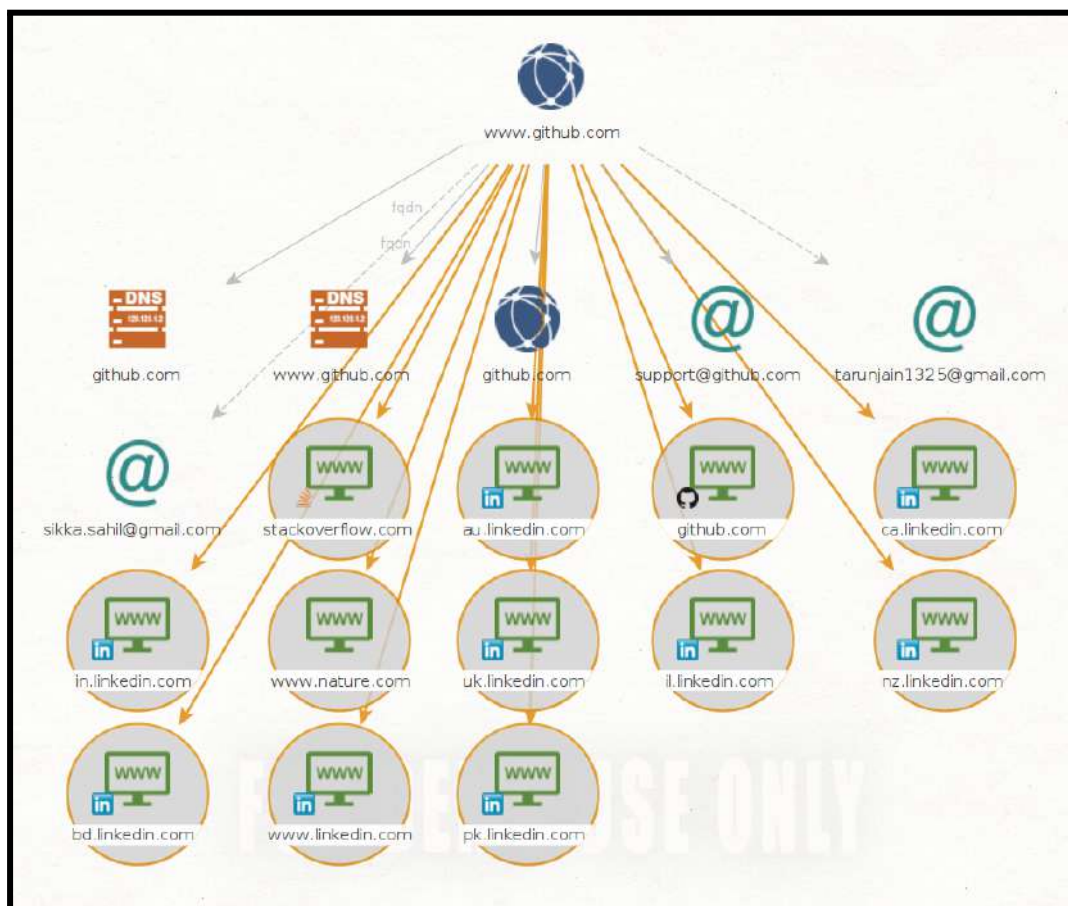

When search for Domains of www.github.com :

When we Search for DNS Names :

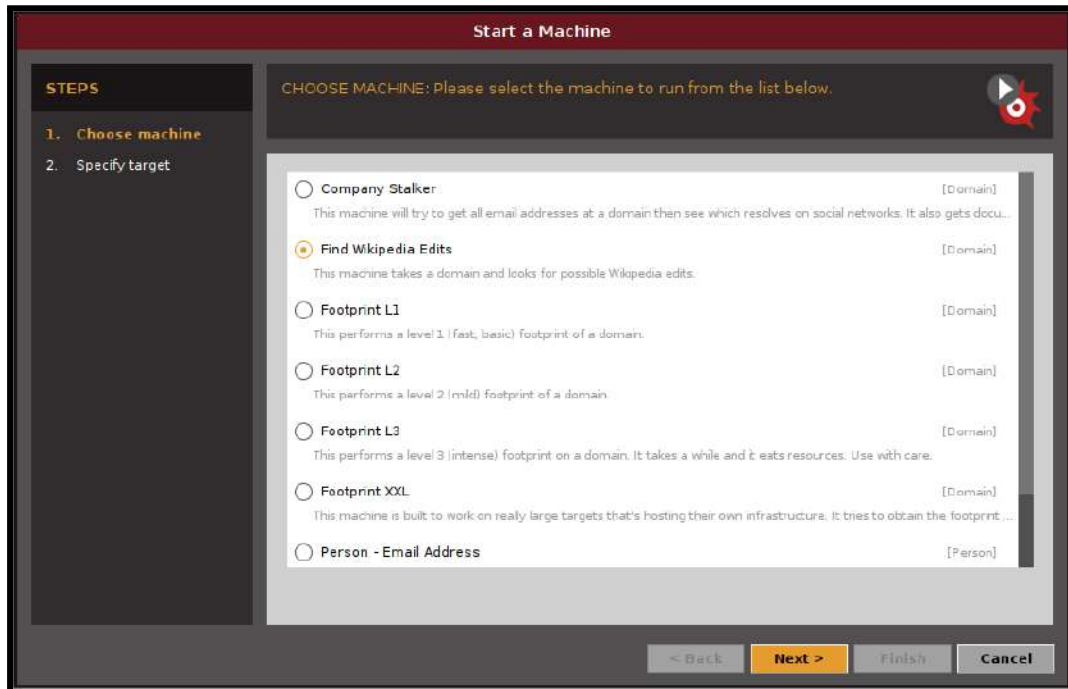**When we Search for Email Address [using Search Engines] on www.github.com**

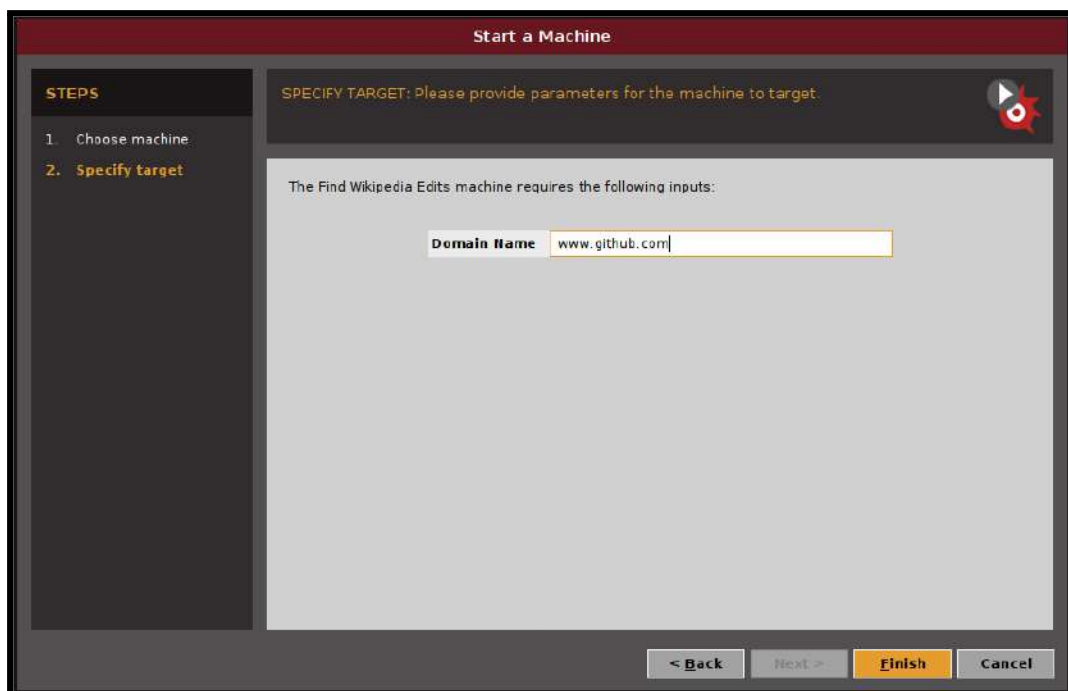**When we Search for Websites Mentioning Domain on www.github.com :**

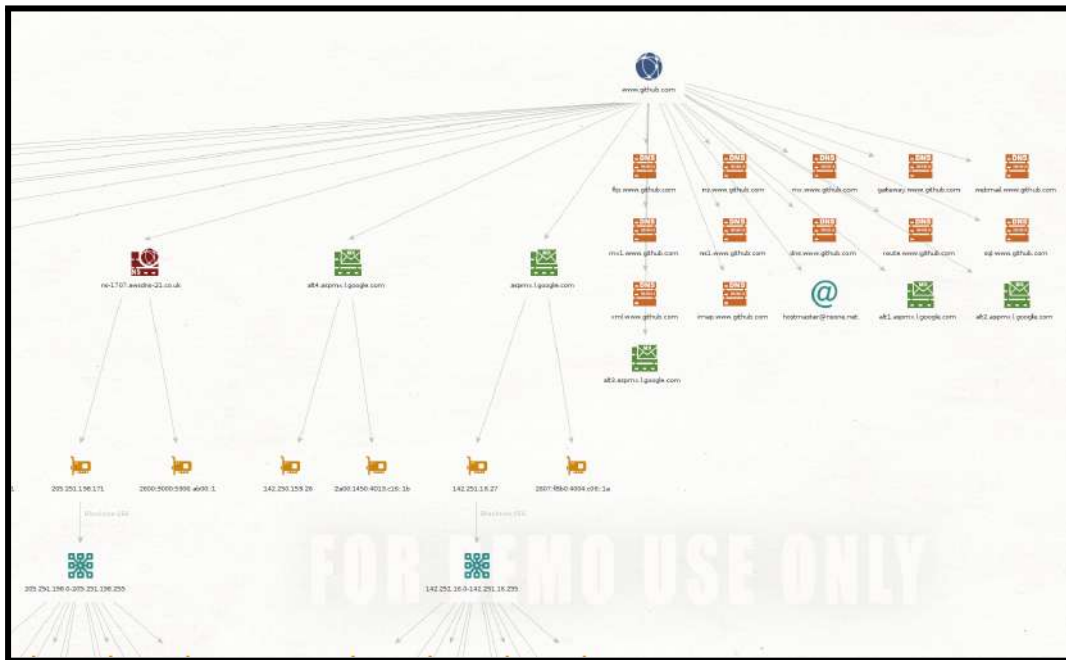**Steps to Start a Machine for Information Gathering [Find Wikipedia Edits]:**

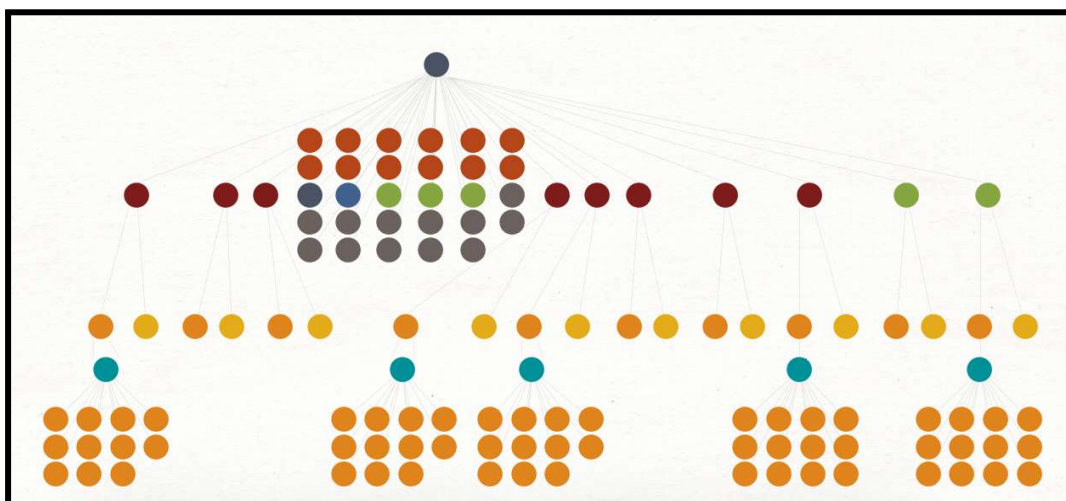**Step 1 :** We will choose the Find Wikipedia Edits machine that we will use.

Step 2 : We will define our target domain name

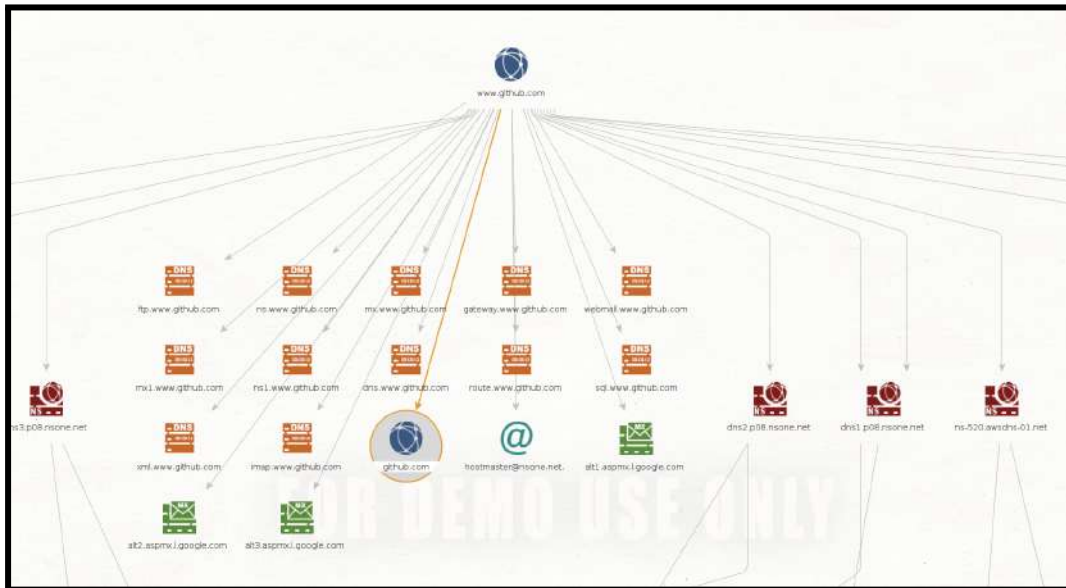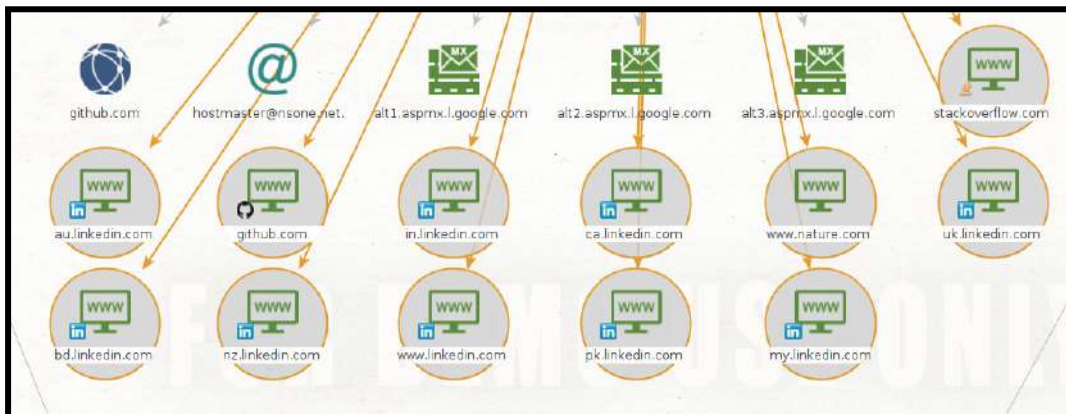**Step 3 :** We will get the following graph for the given Domain

Graph :

Different Node Representation :
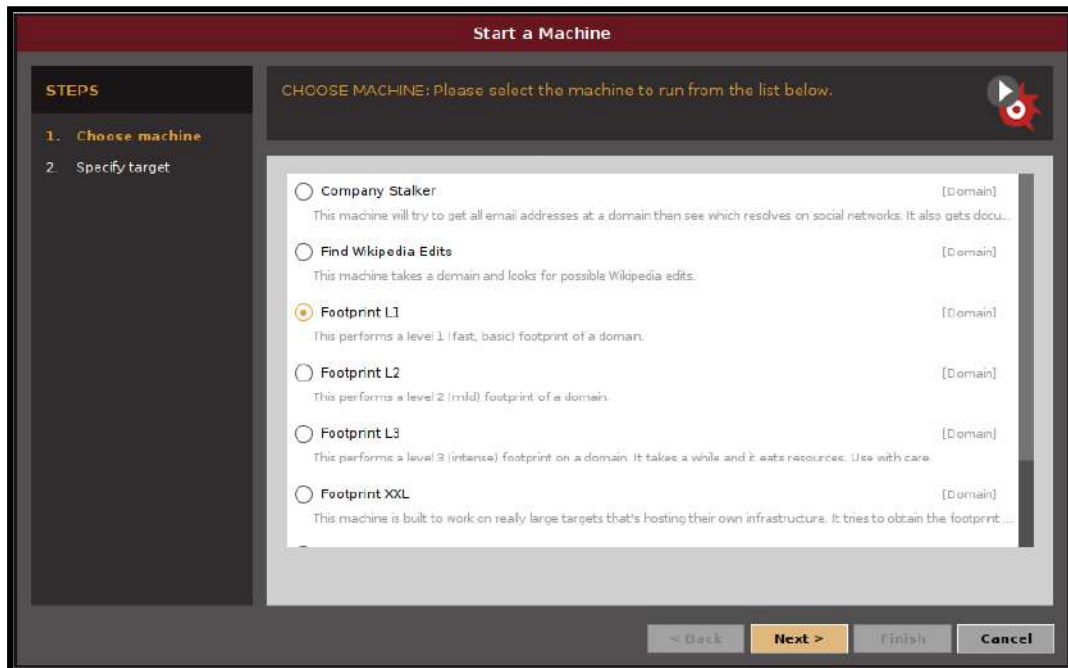
When we Search for Domain :

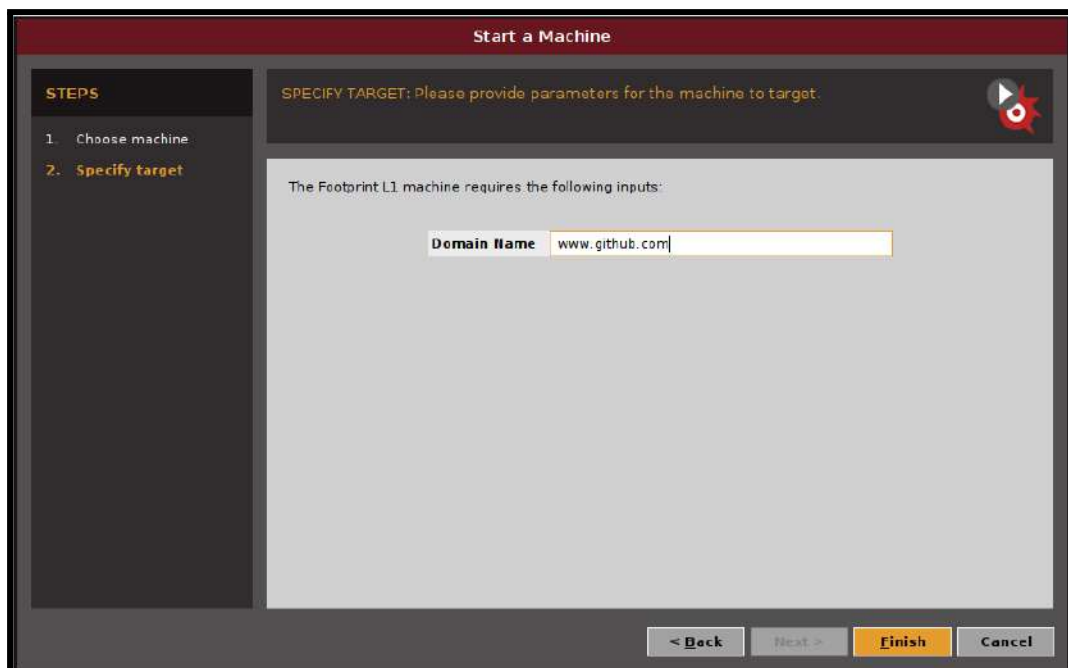**When we search for Websites for www.github.com :**

Steps to Start a Machine for Information Gathering [Footprint L1]:
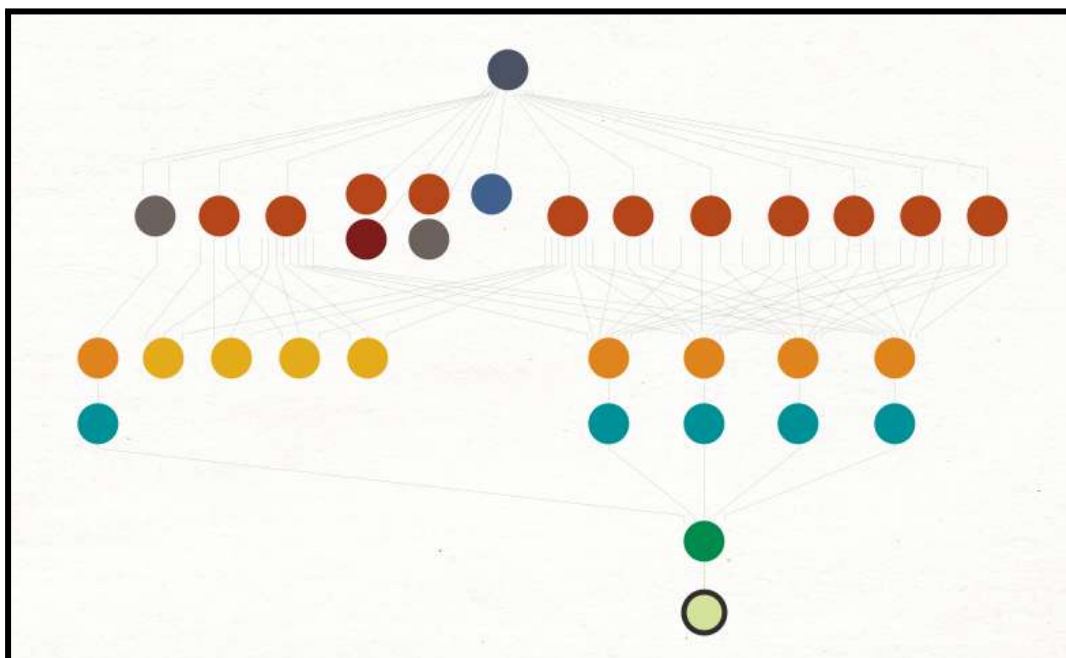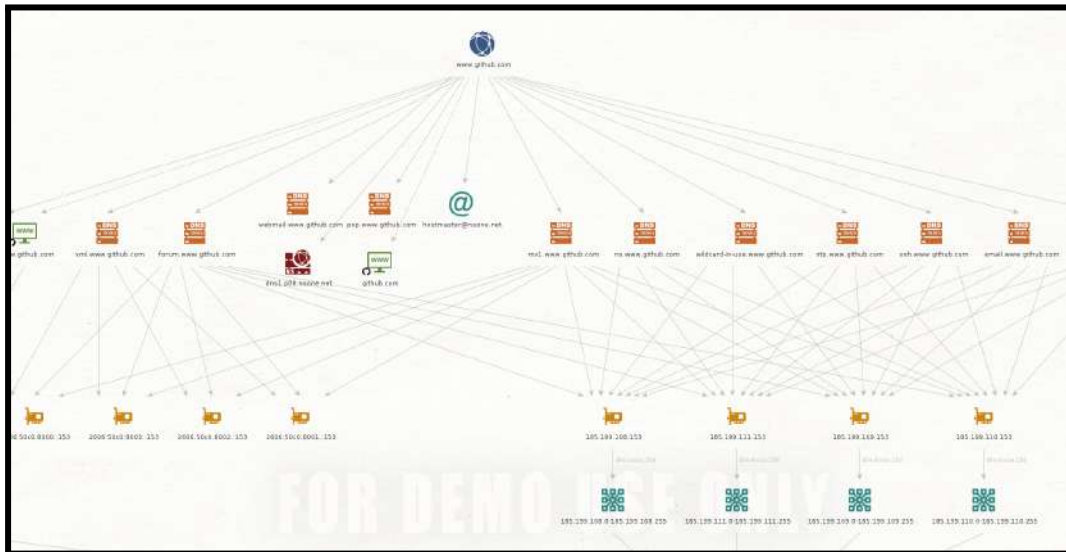
Step 1 : We will choose the Footprint L1 machine that we will use.

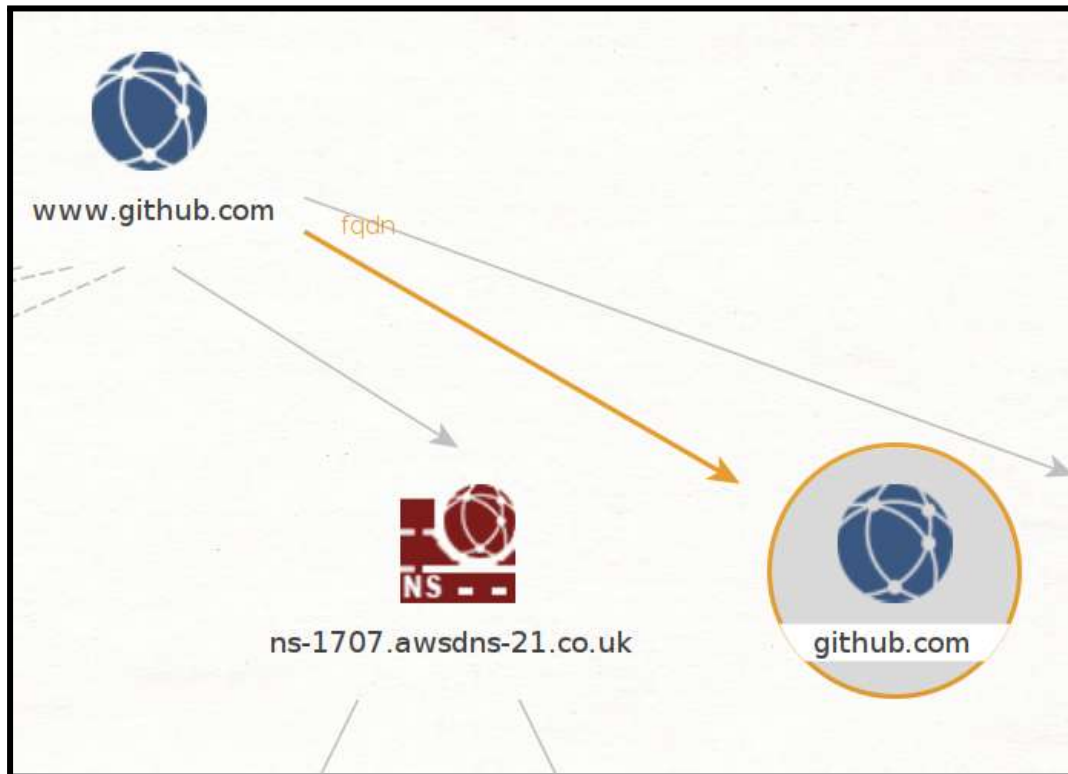**Step 2 :** We will define our target domain name

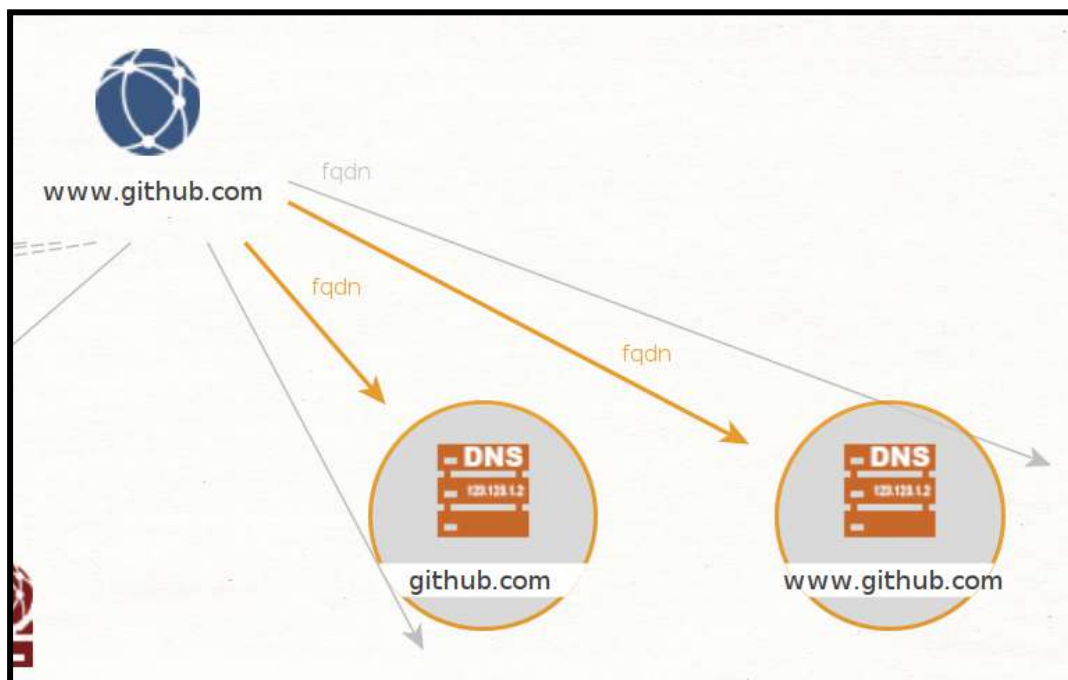**Step 3 :** We will get the following graph for the given Domain
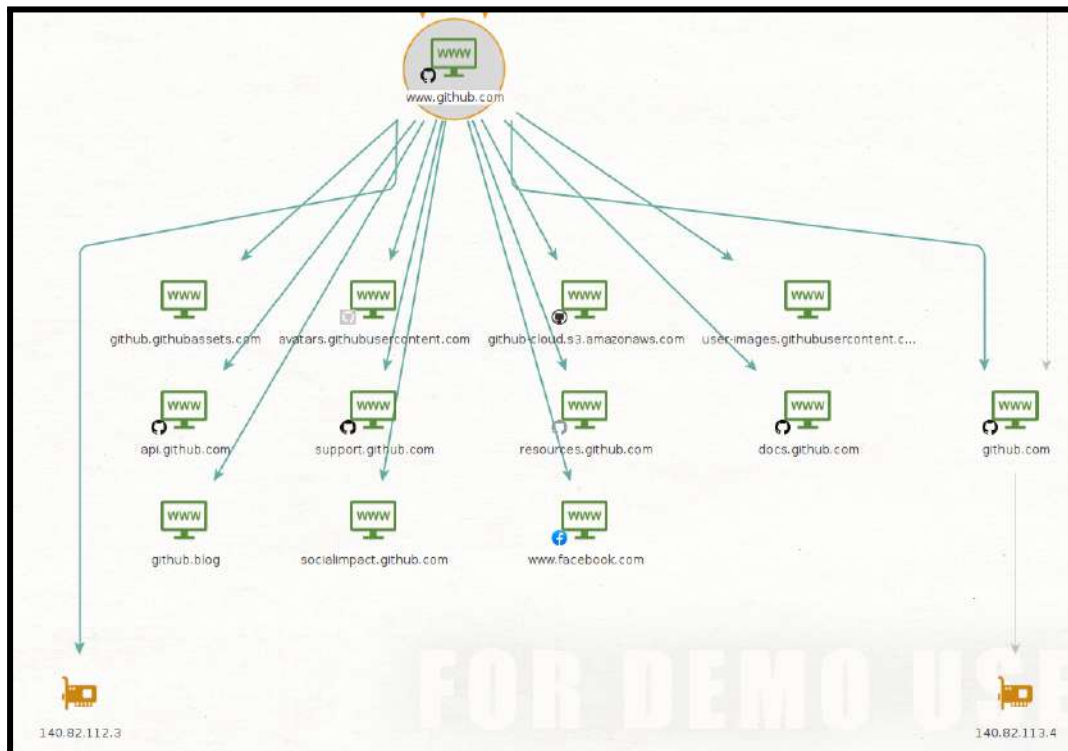

Different Node Representation :

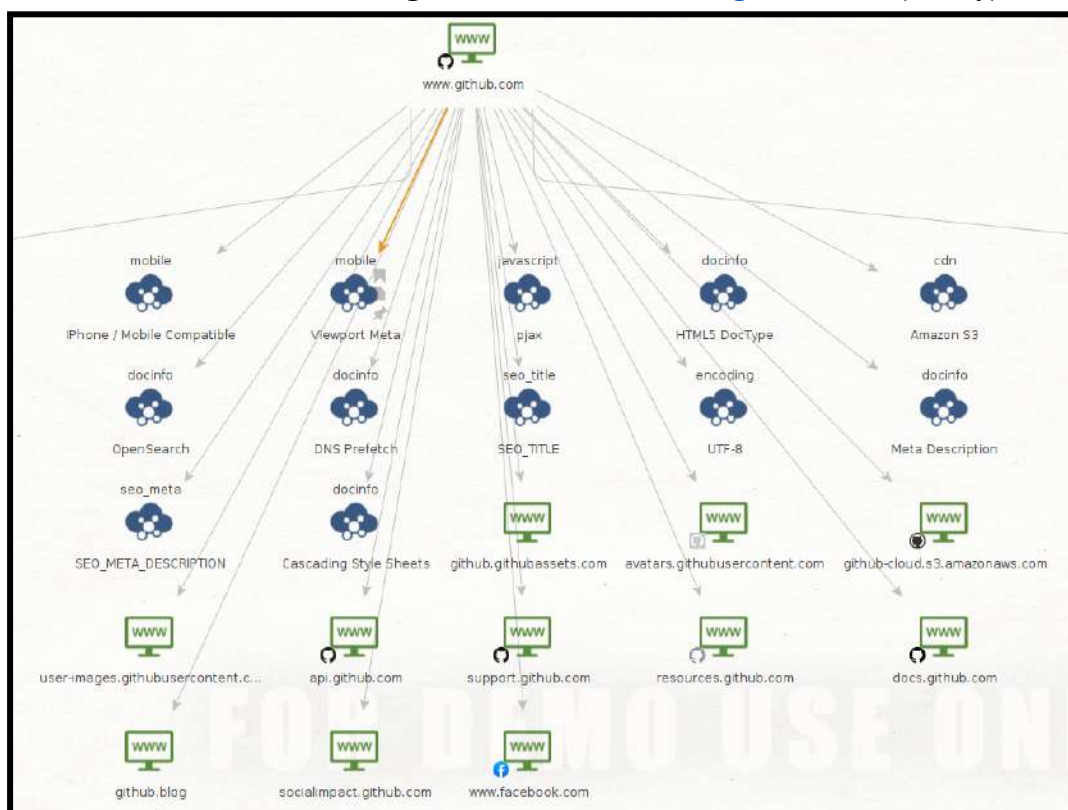**When search for Domains of www.github.com :**
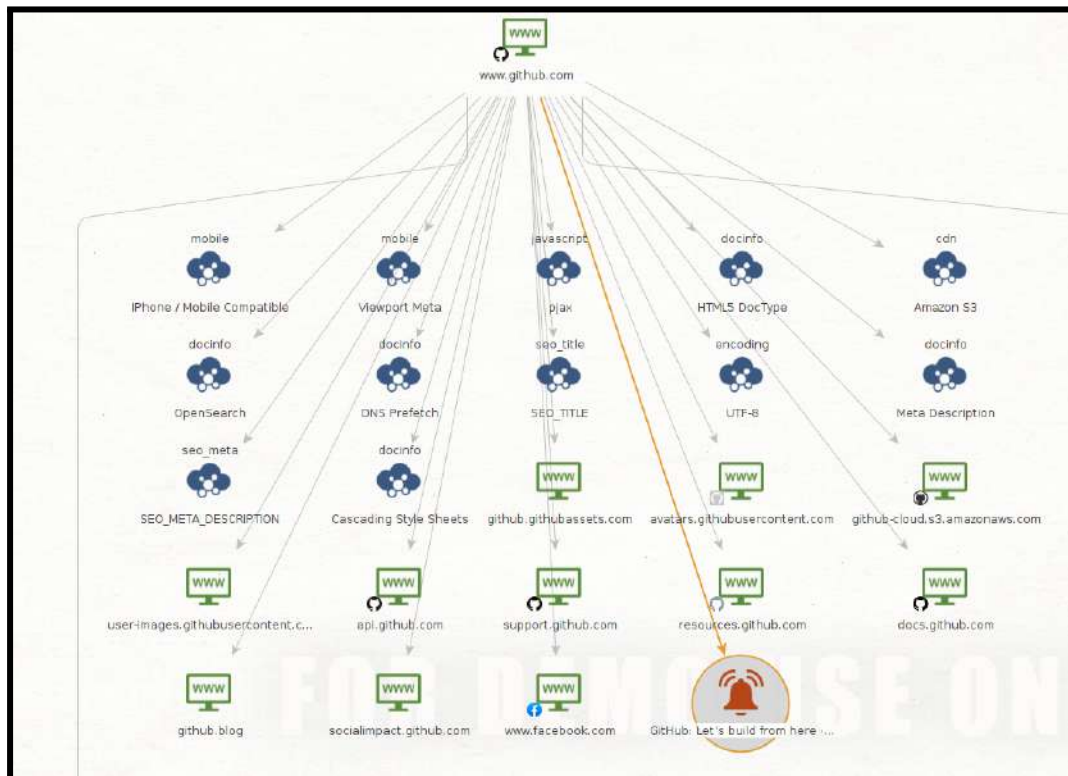

When we Search for DNS Names :

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

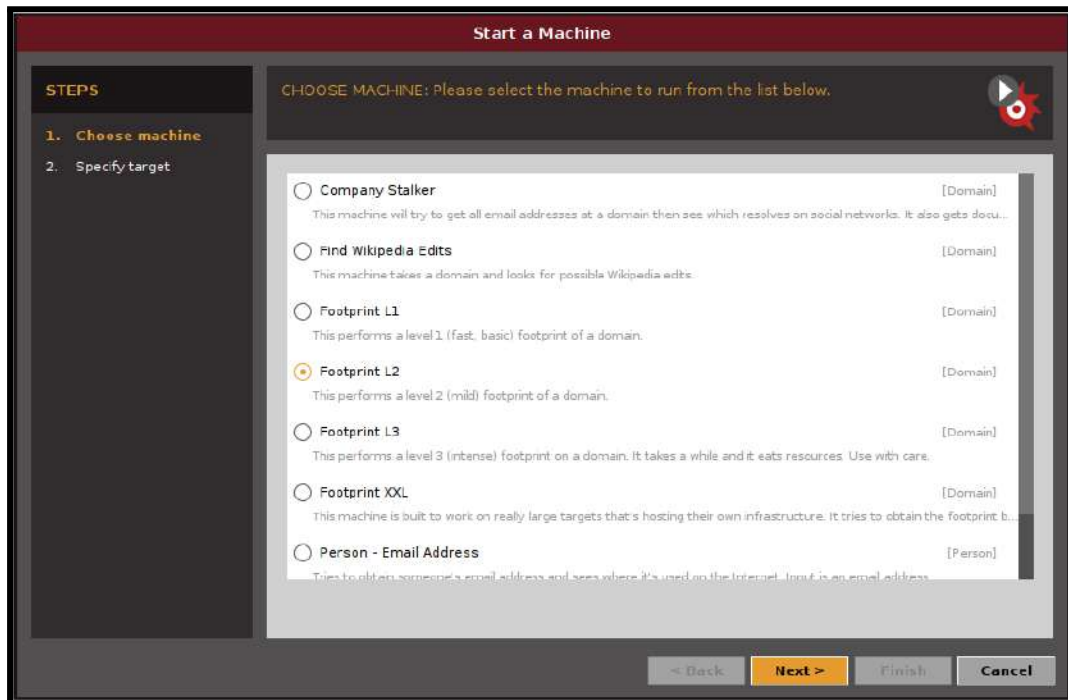**When we Search for Technologies Built With on www.github.com (Entity):**

When we Search for Website Title on www.github.com (Entity):
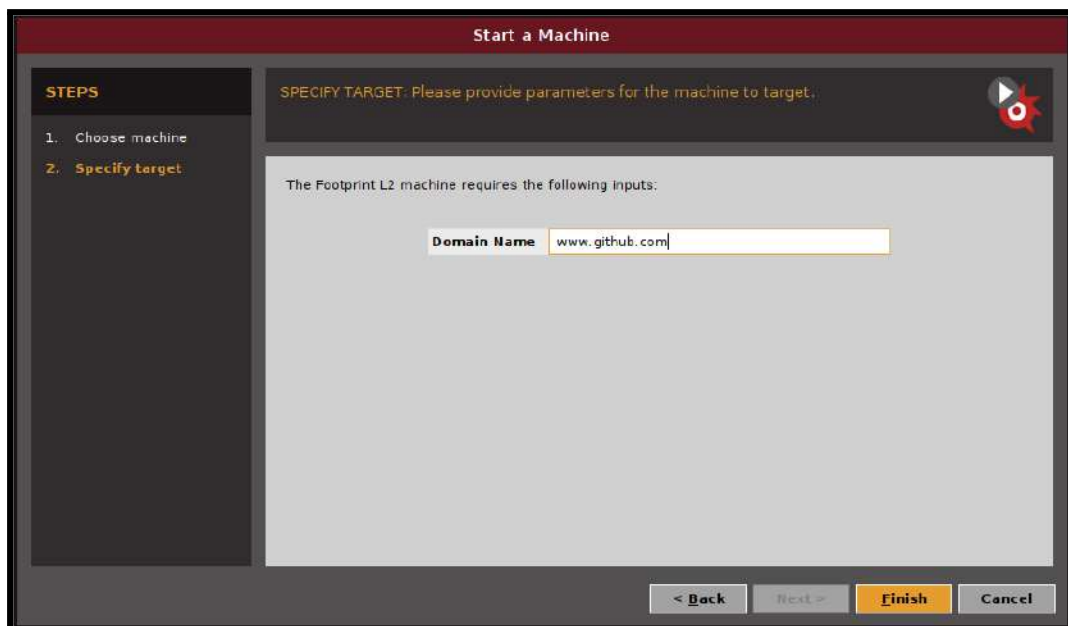
Steps to Start a Machine for Information Gathering [Footprint L2]:
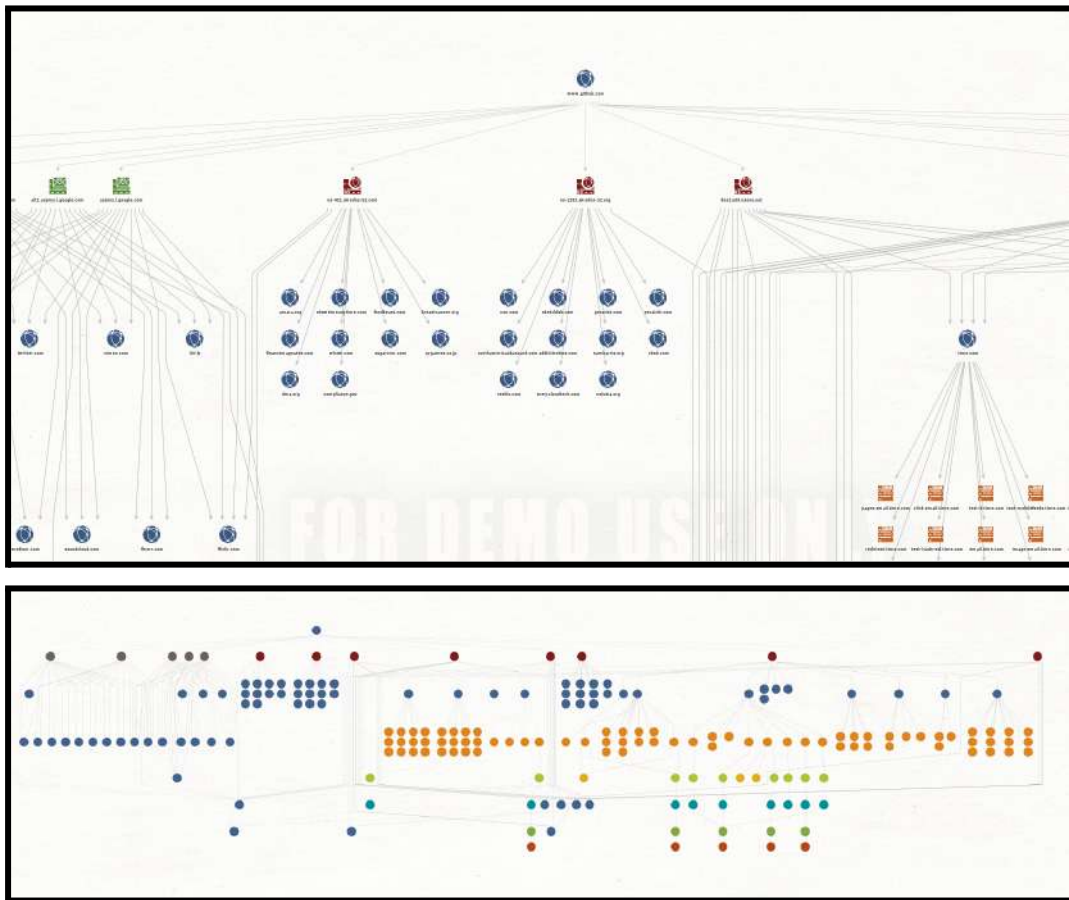
Step 1 : We will choose the Footprint L2 machine that we will use.

Step 2 : We will define our target domain name
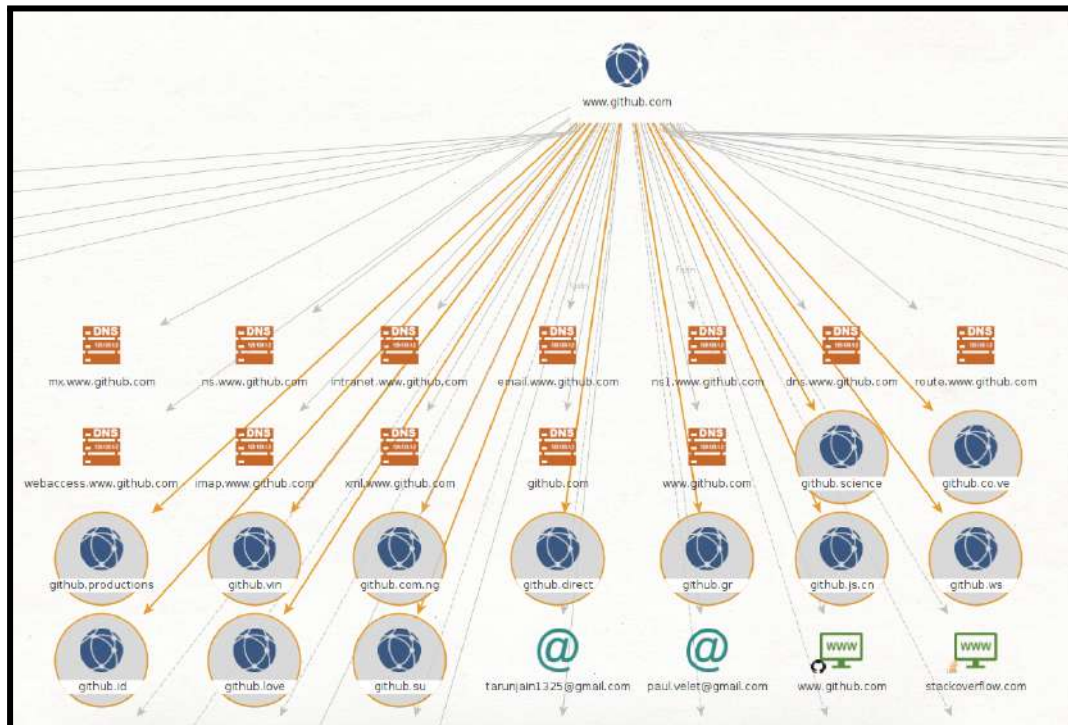
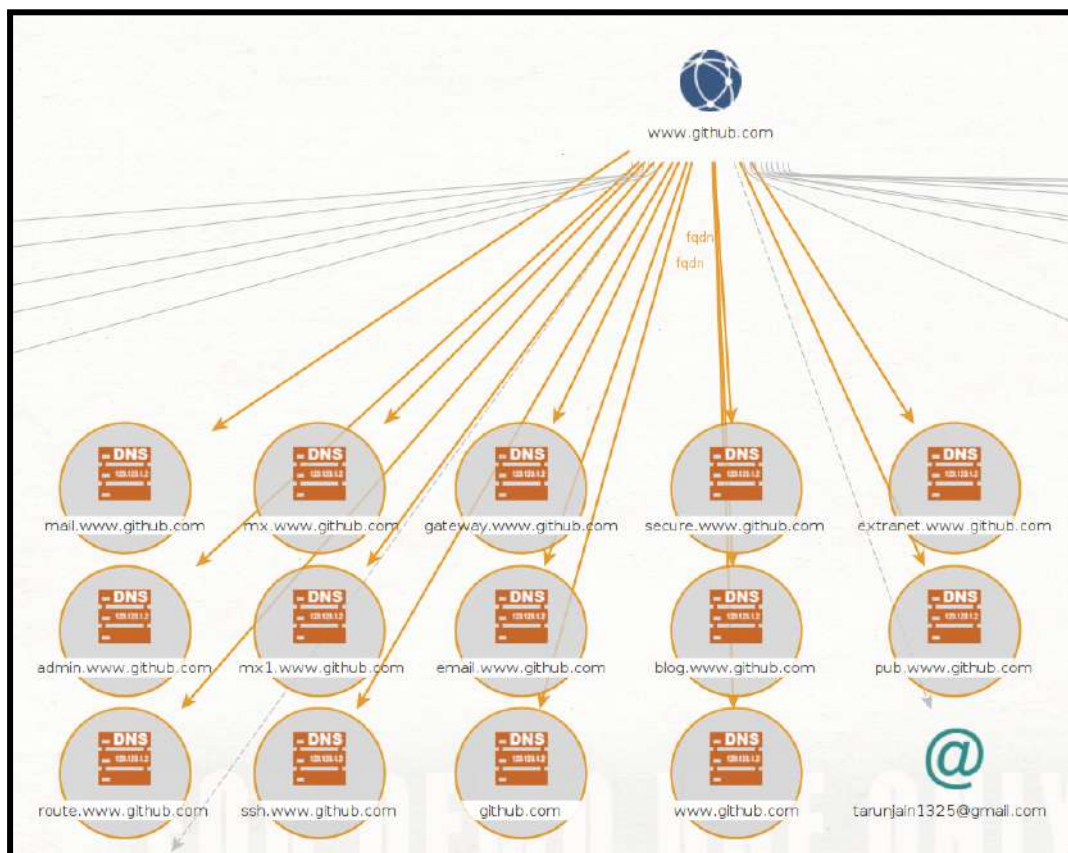**Step 3 :** We will get the following graph for the given Domain
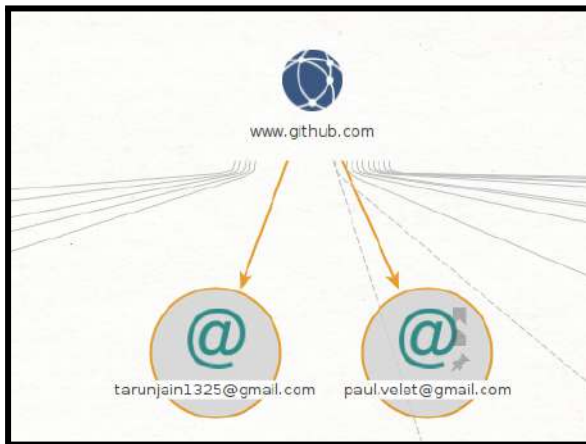

Different Node Representation :

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 :