

PRACTICAL – 2

Aim: Labs for Footprinting and Reconnaissance

1. Open-Source Information Gathering using Windows Command Line Utilities.

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

1. Whether the host is alive or not?
2. Find the IP address of <http://www.certifiedhacker.com>
3. Round Trip Time 4. TTL value 5. Packet loss statistics

```
C:\Users\SHERE>ping www.certifiedhacker.com

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=459ms TTL=52
Reply from 162.241.216.11: bytes=32 time=402ms TTL=52
Reply from 162.241.216.11: bytes=32 time=588ms TTL=52
Reply from 162.241.216.11: bytes=32 time=533ms TTL=52

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 402ms, Maximum = 588ms, Average = 495ms
```

B. Do Tracert / traceroute (command) and gather information related to number of hops between source and destination, response time and other related information.

```
C:\Users\SHERE>tracert www.facebook.com

Tracing route to star-mini.c10r.facebook.com [2a03:2880:f358:1:face:b00c:0:25de]
over a maximum of 30 hops:
  0  0 ms  0 ms  0 ms  2409:4041:6e0f:9ab3::ab
  1  *      *      *      Request timed out.
  2  *      *      *      Request timed out.
  3  101 ms 48 ms 85 ms 2405:200:323:eeee:20::340
  4  36 ms 36 ms 37 ms 2405:200:801:2d00::114
  5  *      *      *      Request timed out.
  6  *      *      *      Request timed out.
  7  42 ms 56 ms 48 ms ae22.pr04.bom1.tfbnw.net [2620:0:1cff:dead:beef::9be]
  8  44 ms 38 ms 47 ms po208.asw03.bom2.tfbnw.net [2620:0:1cff:dead:beef::9874]
  9  47 ms 66 ms 44 ms po256.psw01.bom2.tfbnw.net [2620:0:1cff:dead:beef::97a1]
 10  55 ms 51 ms 46 ms be1.msw1af.04.bom2.tfbnw.net [2a03:2880:f0a4:ffff::60b]
 11  87 ms 41 ms 39 ms edge-star-mini6-shv-04-bom2.facebook.com [2a03:2880:f358:1:face:b00c:0:25de]

Trace complete.
```

C. Do nslookup and gather information.(nslookup is a command-line tool to discover the IP address or DNS record of a specific domain name. It also allows for reverse DNS lookup, letting you find the domain attached to an IP address. To use the tool, enter “nslookup” into the Command Prompt or Terminal.)

```
C:\Users\SHERE>nslookup www.google.com
Server:    UnKnown
Address:   192.168.242.175

Non-authoritative answer:
Name:      www.google.com
Addresses: 2404:6800:4009:82d::2004
           142.250.71.100
```

D. Perform on Net utility: <https://centralops.net/> and gather information.

Domain Dossier Investigate domains and IP addresses

domain or IP address

gnu.ac.in

☒ domain whois record

☒ DNS records

☒ traceroute

☒ network whois record

☒ service scan

go

user: anonymous [157.32.219.228]

balance: 45 units

[log in](#) | [account info](#)

To obtain Whois data redacted because of the [GDPR](#) or privacy services, try ICANN's RDRS. [\[more information\]](#)

Address lookupcanonical name [gnu.ac.in.](#)

aliases

addresses [35.154.251.128](#)**Domain Whois record**Queried [whois.registry.in](#) with "gnu.ac.in"...

Domain Name: gnu.ac.in
Registry Domain ID: D3325598-IN
Registrar WHOIS Server:
Registrar URL: <http://www.ernet.in>
Updated Date: 2024-02-04T07:03:42Z
Creation Date: 2009-03-04T06:28:40Z
Registry Expiry Date: 2033-03-04T06:28:40Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:

2. Do the netcraft and gather the information. (Provides information about other websites, including details like IP address, web server OS, and DNS server.)

[LEARN MORE](#) [REPORT FRAUD](#)

Site report for <http://www.google.com>

► 🔍 Look up another site?

Share:

Background

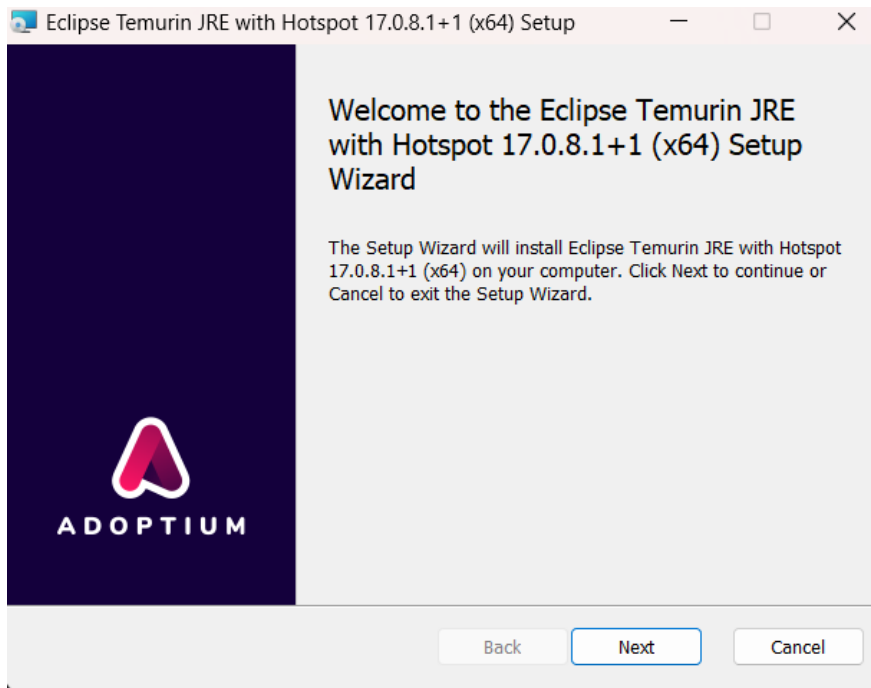
Site title	Google	Date first seen	November 1998
Site rank	1	Primary language	English
Description	Search the world's information, including webpages, images, videos and more. Google has many special features to help you find exactly what you're looking for.		

Network

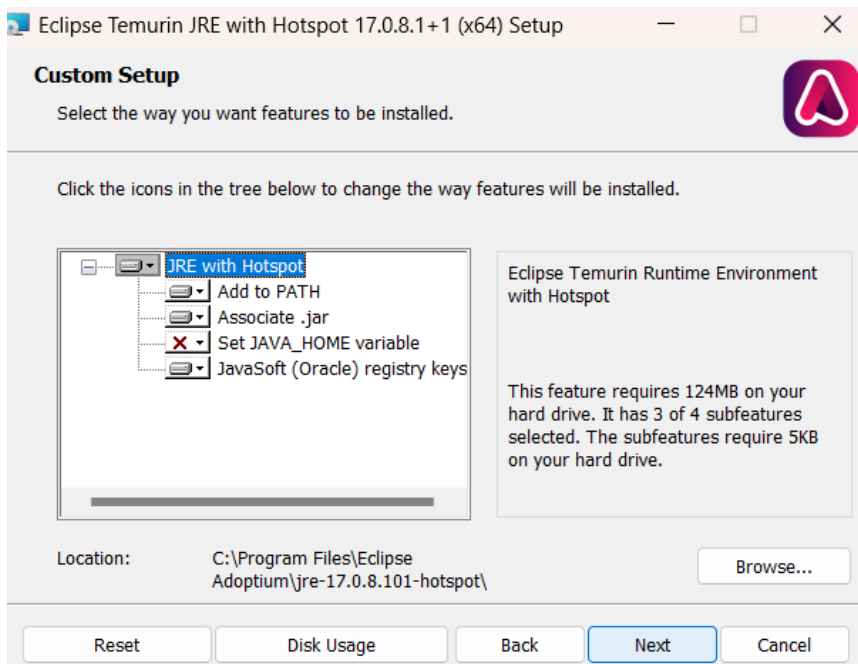
Site	http://www.google.com	Domain	google.com
Netblock Owner	Google LLC	Nameserver	ns1.google.com

3. Gather the information using MALTEGO Tool.

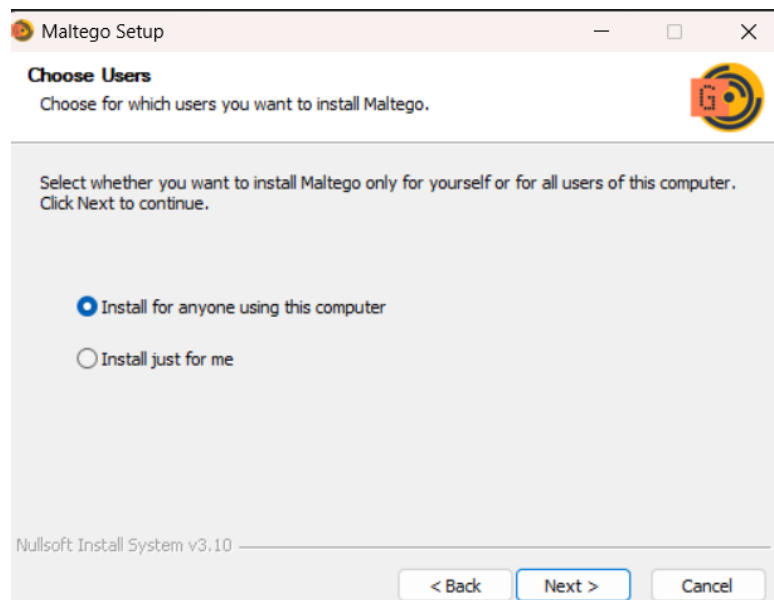
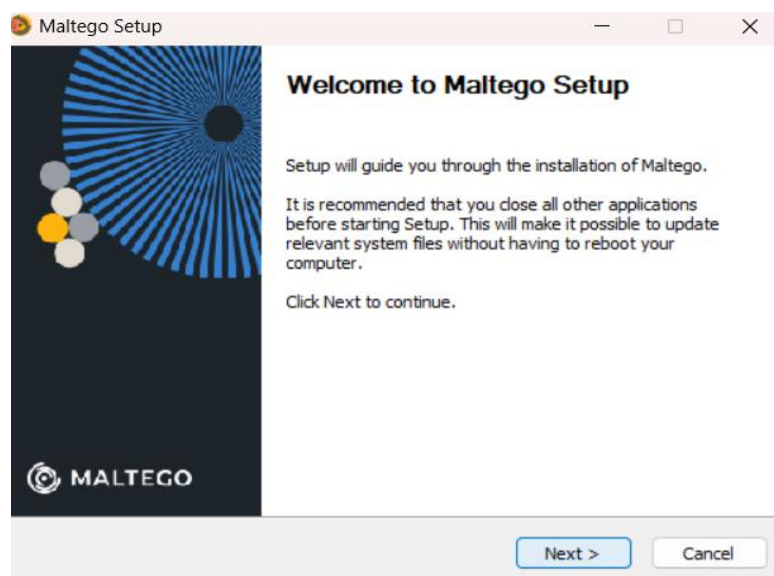
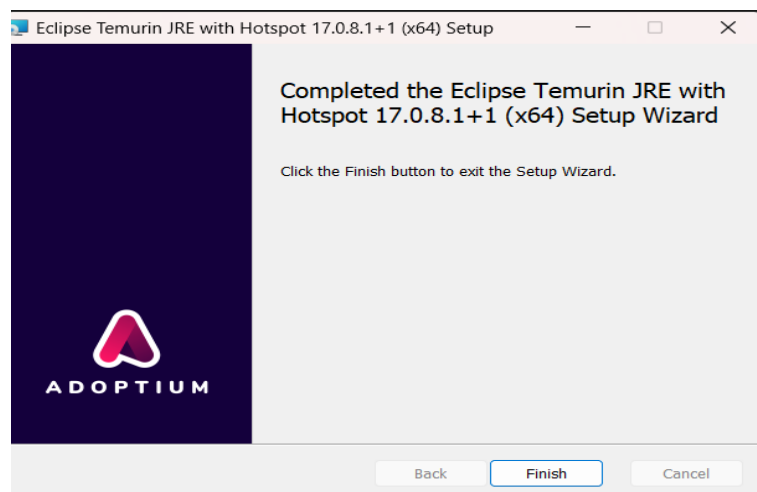
- ❖ Installation of Maltego :
- click and execute the Maltego Software .exe file.

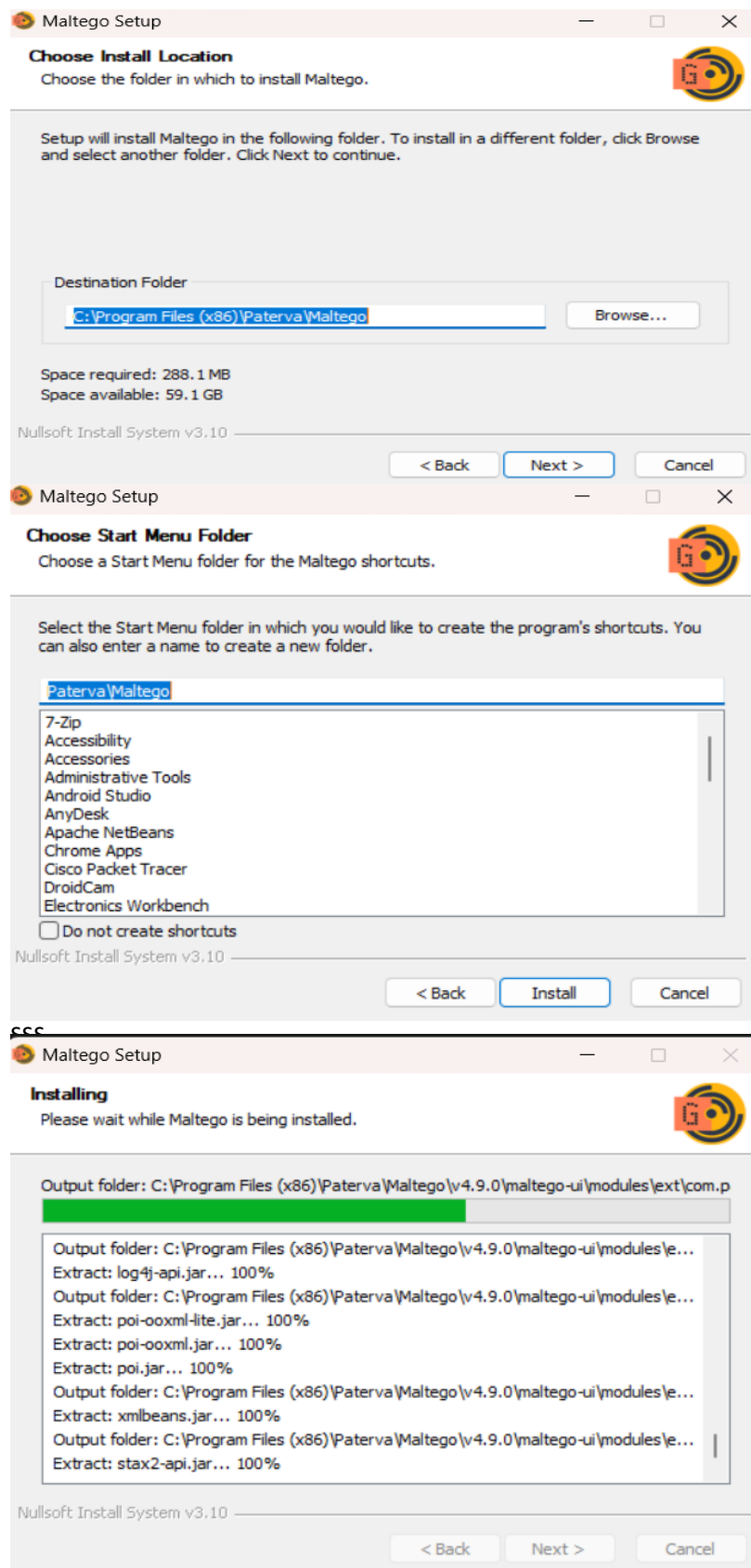


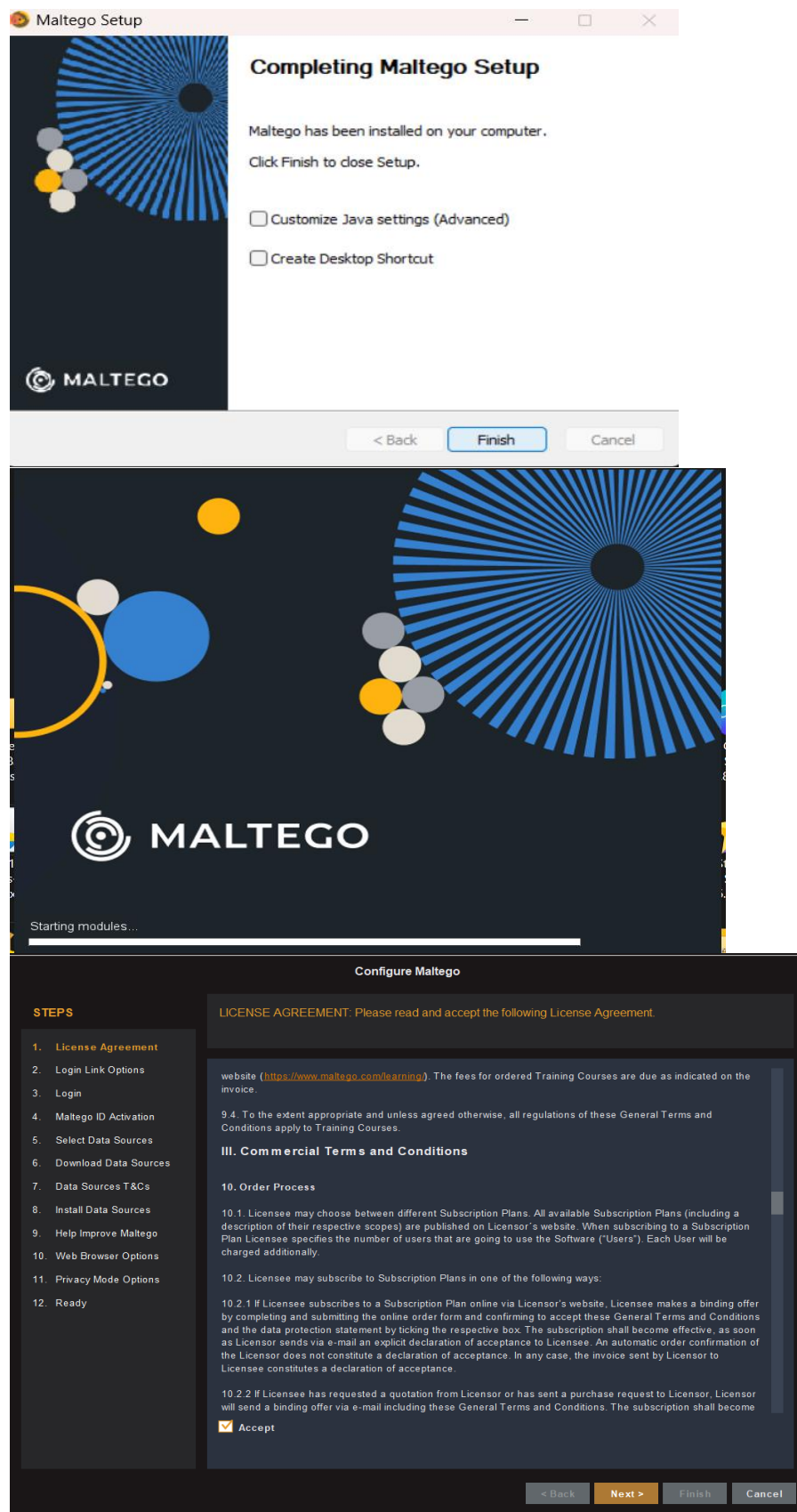
- The Maltego is based on the JAVA so it will need the JRE so click next if already installed.

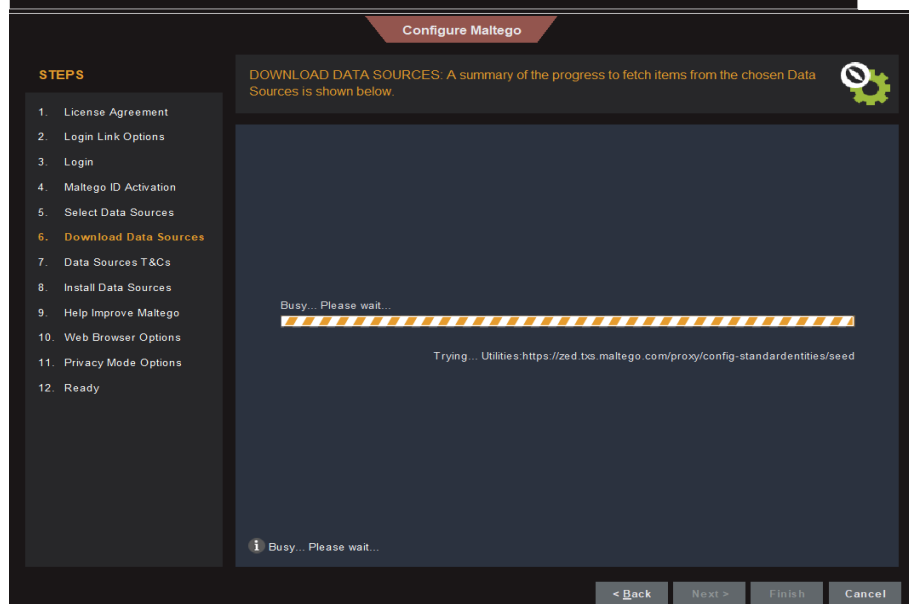
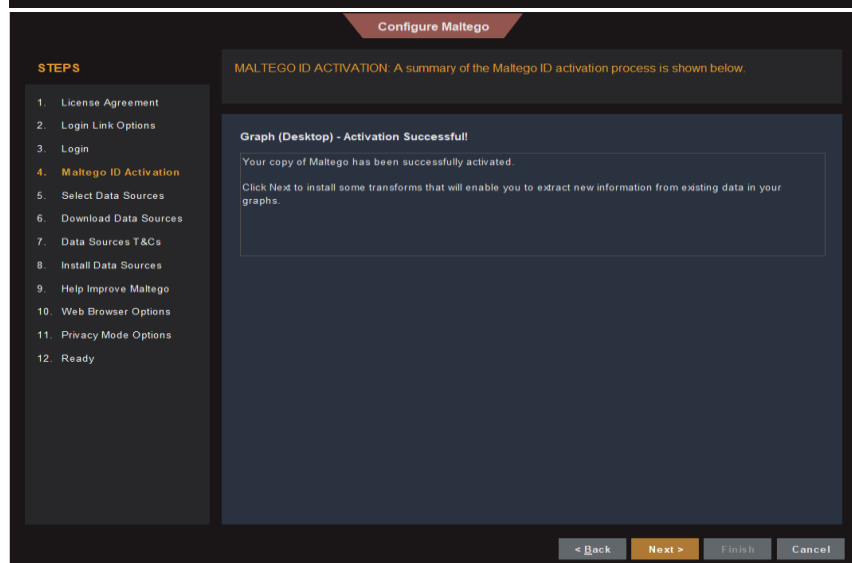
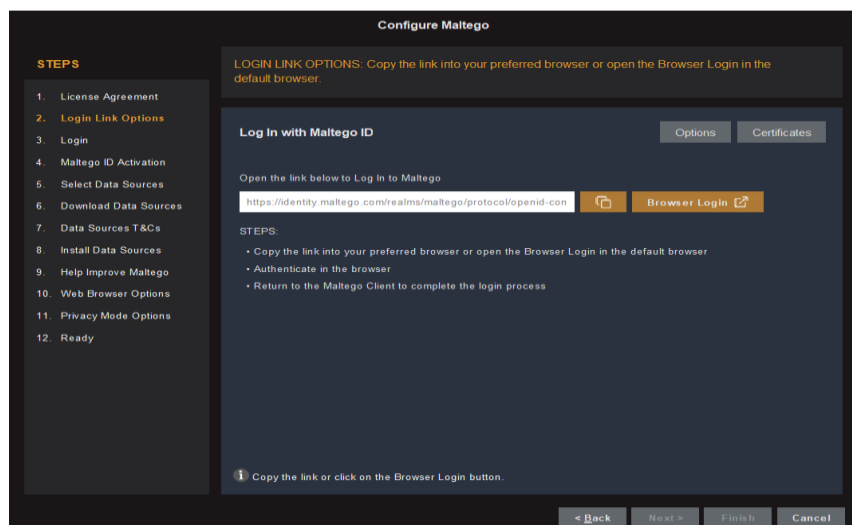


- As it Goes to further step click next.

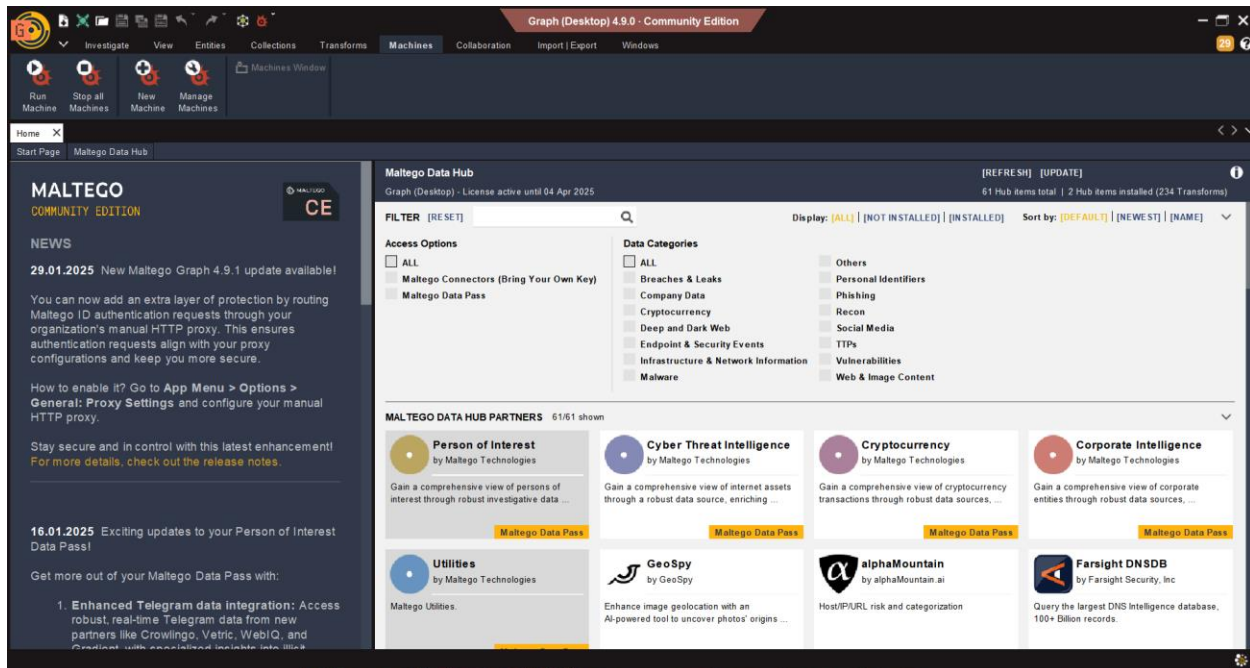




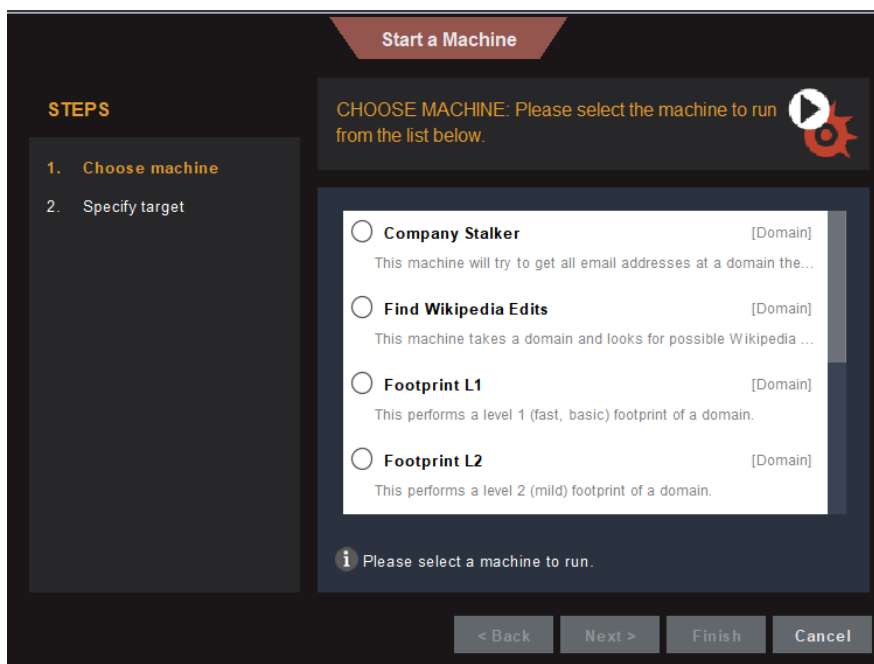




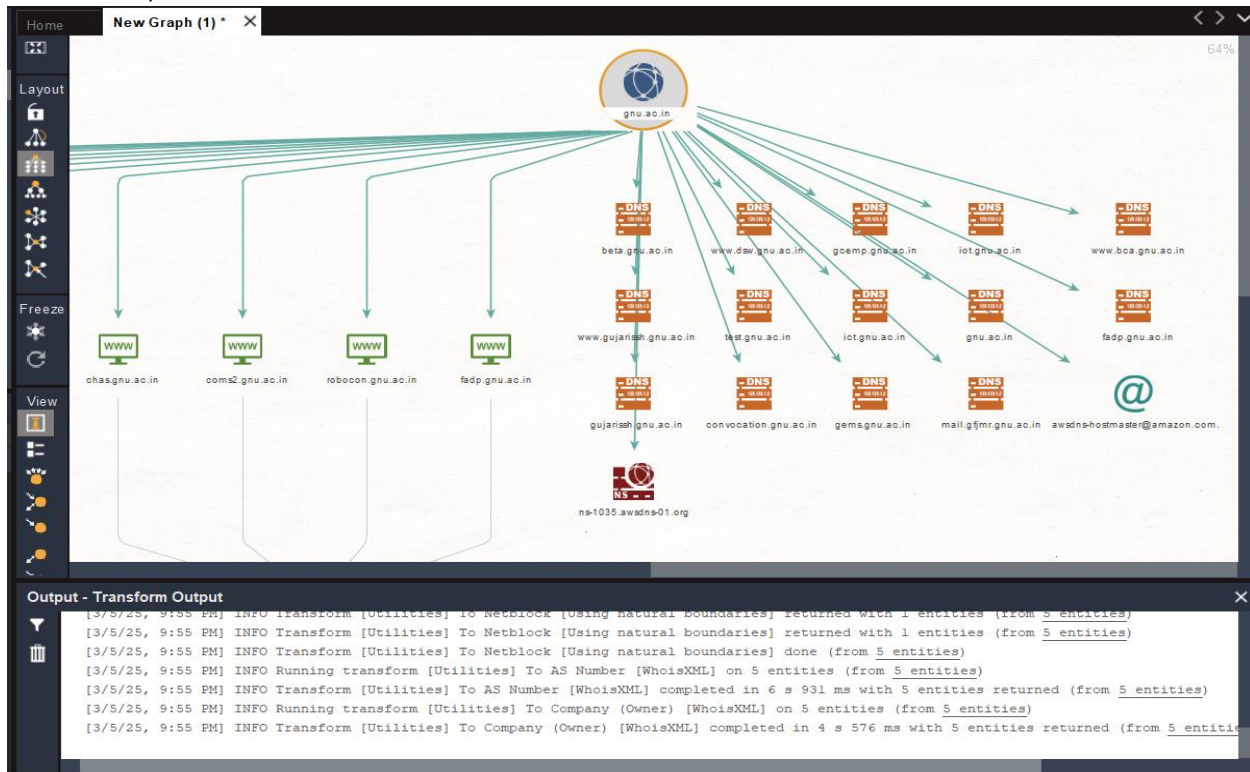
- After completing all the step one by one you will redirected to the Home page of Maltego.
- Where next step will be go to the machine and select option of run machine it will ask few details about the machine like : name for the machine , on which domain you want to us machine e.x. gnu.ac.in (then it will create a parent node of this domain name and then start searching the information about that particular domain like its sub domain's , Hosting, Server etc.)



- After clicking on the run server you have to select the machine type for example here we have selected the "Footprinting L1" machine for the working.



- Here Is the Details about the Particular Domain (in our case “gnu.ac.in”) like about its servers, sub domains etc.



4. Finding Company's Sub-domains using "Sublist3r" (Kali Linux) and "snrublist3r" (Kali Linux/Windows).

- Installing the snrublist3r on Kali
- Open Terminal in Kali
- Command: git clone <https://github.com/b3n-i4m1n/snrublist3r.git>

```
(kali@kali)-[~]
$ git clone https://github.com/b3n-j4m1n/snrublist3r.git
Cloning into 'snrublist3r' ...
remote: Enumerating objects: 112, done.
remote: Counting objects: 100% (112/112), done.
remote: Compressing objects: 100% (69/69), done.
remote: Total 112 (delta 48), reused 105 (delta 41), pack-reused 0 (from 0)
Receiving objects: 100% (112/112), 15.24 MiB | 1.99 MiB/s, done.
Resolving deltas: 100% (48/48), done.
```

- Setup the Environment for sunrublist3r and activate it.
- Command : 1) `cd snrublist3r` 2) `python -m venv snrublist3r`
3) `source ./snrublist3r/bin/activate`

```
(kali㉿kali)-[~]  
$ cd snrublist3r  
  
(kali㉿kali)-[~/snrublist3r]  
$ python -m venv snrublist3r  
  
(kali㉿kali)-[~/snrublist3r]  
$ source ./snrublist3r/bin/activate
```

- Install the Requirements for snrublist3r
- Command : `pip install -r requirements.txt`

```
(snrublist3r)-(kali㉿kali)-[~/snrublist3r]
└─$ pip install -r requirements.txt

Collecting aiodns (from -r requirements.txt (line 1))
  Downloading aiodns-3.2.0-py3-none-any.whl.metadata (4.0 kB)
Collecting beautifulsoup4 (from -r requirements.txt (line 2))
  Downloading beautifulsoup4-4.13.3-py3-none-any.whl.metadata (3.8 kB)
Collecting colorama (from -r requirements.txt (line 3))
  Downloading colorama-0.4.6-py2.py3-none-any.whl.metadata (17 kB)
Collecting lxml (from -r requirements.txt (line 4))
  Downloading lxml-5.3.0-cp312-cp312-manylinux_2_28_x86_64.whl.metadata (3.8 kB)
```

- After performing all the given step now snrublist3r is ready to perform the domain searching
- Command: `python snrublist3r.py -d gnu.ac.in`
- we can use the multiple parameters like `-v` for verbose mode, `- fast` for fast mode etc.

```
(snrublist3r)-(kali@kali)-[/snrublist3r]
$ python snrublist3r.py -d gnu.ac.in -v


      .--.
     /  __ \
    /   /  )
   /___/  /
  /_____/

[+] snrubbing starting for gnu.ac.in
[*] starting source scraper for sources ['AlienVault', 'Anubis', 'Ask', 'Bing', 'Certificate Search', 'Common Crawl', 'Digitorus', 'DNSDumpster', 'DuckDuckGo', 'Gist', 'Google',
rusTotal', 'Wayback Machine', 'Yahoo']
[*] starting AlienVault query...
[+] test.gnu.ac.in [AlienVault]
[+] chas.gnu.ac.in [AlienVault]
[+] cpcontacts.robocon.gnu.ac.in [AlienVault]
[+] cpcontacts.manthan.gnu.ac.in [AlienVault]
[+] iot.gnu.ac.in [AlienVault]
[+] www.aaghaz.gnu.ac.in [AlienVault]
[+] ce.gnu.ac.in [AlienVault]
[+] cpcalendars.support.gnu.ac.in [AlienVault]
[+] cpcontacts.chas.gnu.ac.in [AlienVault]
[+] marine.gnu.ac.in [AlienVault]
[+] www.coms2.gnu.ac.in [AlienVault]
[+] manthan.gnu.ac.in [AlienVault]
[+] www.chas.gnu.ac.in [AlienVault]
[+] betaampics.gnu.ac.in [AlienVault]
[+] www.gnu.ac.in [AlienVault]
[+] www.support.gnu.ac.in [AlienVault]
```

- For the Windows use following steps to perform the sub domain searching.

```
C:\Users\SHERE\OneDrive\Desktop\Ganpat University Work\Sem 6\Ethical Hacking (EH)>git clone https://github.com/b3n-j4m1n/snrublist3r.git
Cloning into 'snrublist3r'...
remote: Enumerating objects: 112, done.
remote: Counting objects: 100% (112/112), done.
remote: Compressing objects: 100% (69/69), done.
remote: Total 112 (delta 48), reused 105 (delta 41), pack-reused 0 (from 0)
Receiving objects: 100% (112/112), 15.24 MiB | 1.15 MiB/s, done.
Resolving deltas: 100% (48/48), done.
```

```
C:\Users\SHERE\OneDrive\Desktop\Ganpat University Work\Sem 6\Ethical Hacking (EH)>cd snrublist3r
C:\Users\SHERE\OneDrive\Desktop\Ganpat University Work\Sem 6\Ethical Hacking (EH)\snrublist3r>python -m venv snrublist3r
C:\Users\SHERE\OneDrive\Desktop\Ganpat University Work\Sem 6\Ethical Hacking (EH)\snrublist3r>. \snrublist3r\Scripts\Activate.ps1
C:\Users\SHERE\OneDrive\Desktop\Ganpat University Work\Sem 6\Ethical Hacking (EH)\snrublist3r>pip install -r requirements.txt
Collecting aiodns (from -r requirements.txt (line 1))
  Downloading aiodns-3.2.0-py3-none-any.whl.metadata (4.0 kB)
Collecting beautifulsoup4 (from -r requirements.txt (line 2))
  Downloading beautifulsoup4-4.13.3-py3-none-any.whl.metadata (3.8 kB)
Requirement already satisfied: colorama in c:\users\shere\AppData\Local\Programs\Python\Python311\Lib\site-packages (from -r requirements.txt (line 3)) (0.4.6)
Collecting lxml (from -r requirements.txt (line 4))
  Downloading lxml-5.3.1-cp311-cp311-win_amd64.whl.metadata (3.8 kB)
Requirement already satisfied: requests in c:\users\shere\AppData\Local\Programs\Python\Python311\Lib\site-packages (from -r requirements.txt (line 5)) (2.32.3)
C:\Users\SHERE\OneDrive\Desktop\Ganpat University Work\Sem 6\Ethical Hacking (EH)\snrublist3r>python snrublist3r.py -d gtu.ac.in -v
```



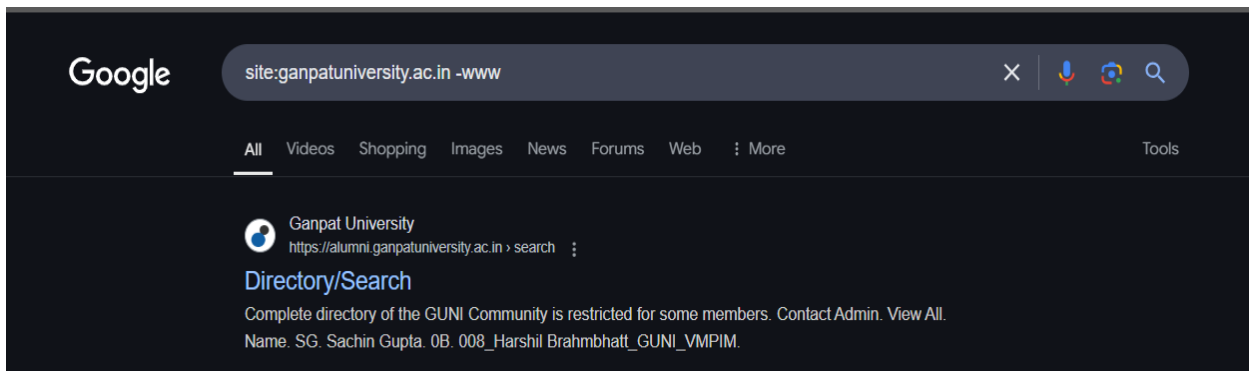
```
snrublist3r

[*] snrubbing starting for gtu.ac.in
[*] starting source scraper for sources ['AlienVault', 'Anubis', 'Ask', 'Bing', 'Certificate Search', 'Common Crawl', 'Digitorus', 'DNSDumpster', 'DuckDuckGo', 'Gist', 'Google', 'Hacker Target', 'RapidDNS', 'VirusTotal', 'Wayback Machine', 'Yahoo']
[*] starting AlienVault query...
[+] set.gtu.ac.in [AlienVault]
[+] www.recruit19t.gtu.ac.in [AlienVault]
[+] staffs.gtu.ac.in [AlienVault]
[+] www.billdesk.gtu.ac.in [AlienVault]
[+] www.affiliation.gtu.ac.in [AlienVault]
[+] www.design.gtu.ac.in [AlienVault]
[+] photo.gtu.ac.in [AlienVault]
[+] www.studentsupport.gtu.ac.in [AlienVault]
[+] www.de.gtu.ac.in [AlienVault]
[+] gsn.gtu.ac.in [AlienVault]
[+] phd_reviewcard.gtu.ac.in [AlienVault]
[+] integratedcourse.gtu.ac.in [AlienVault]
[+] www.result2.gtu.ac.in [AlienVault]
[+] www.100points.gtu.ac.in [AlienVault]
```

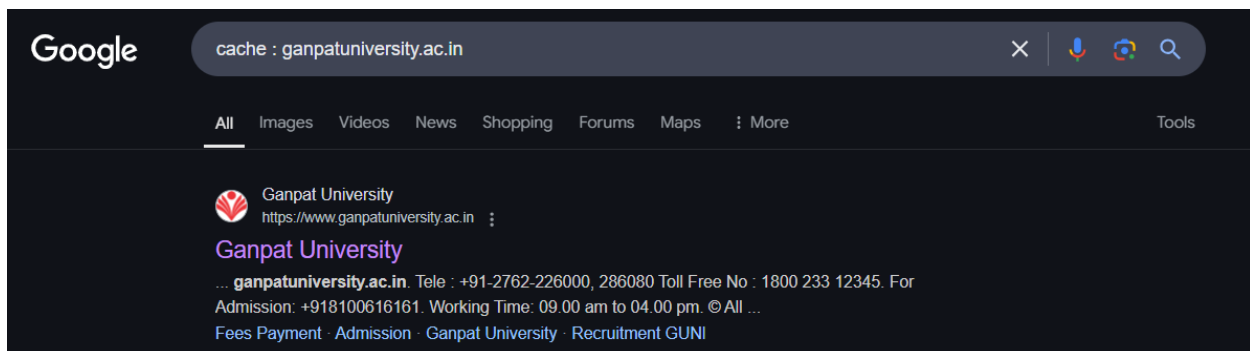
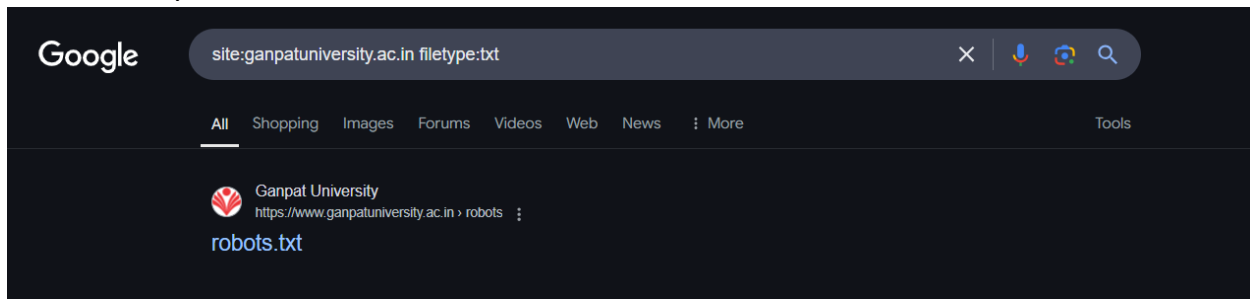
5. Perform following Hacking Techniques using Google Dorks.

A. Find the various information using Google Search Operators.

- The site:ganpatuniversity.ac.in -www query searches for pages on the Ganpat University domain excluding those from "www.ganpatuniversity.ac.in".

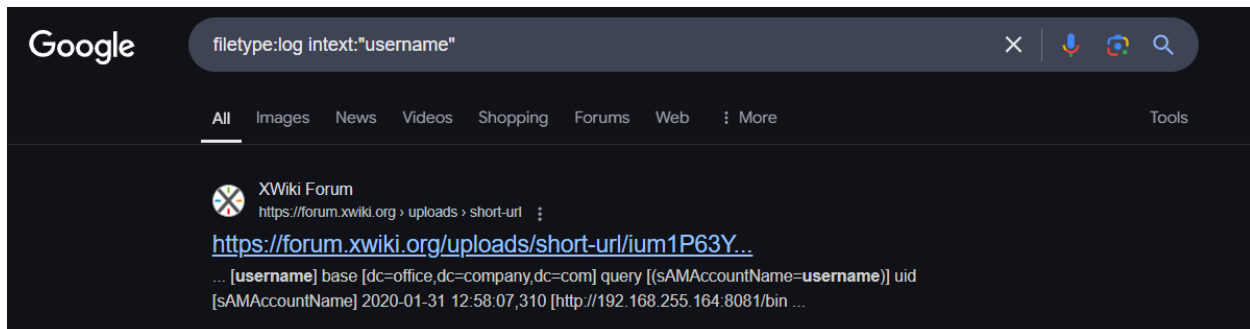


- The query site:ganpatuniversity.ac.in filetype:txt searches for text (.txt) files on the Ganpat University website.



B. Perform any five dorks for the following categories:

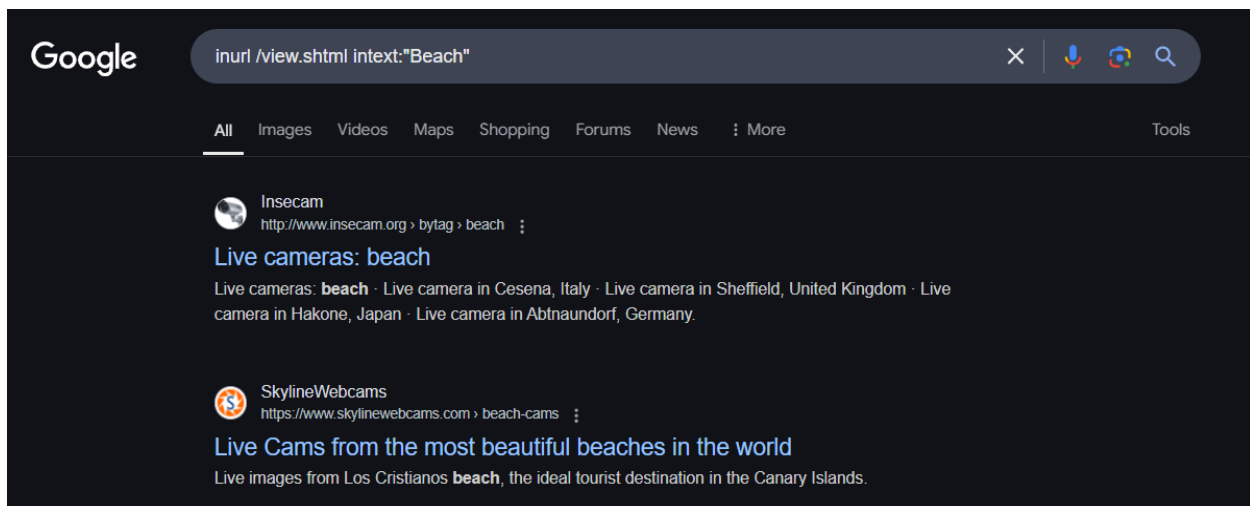
1) Files Containing Usernames



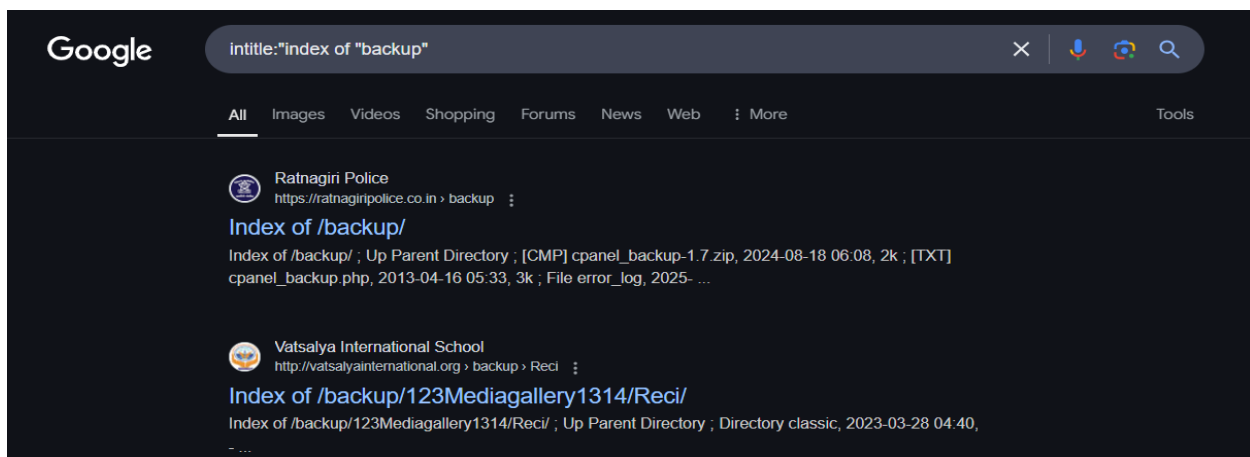
2) Files Containing Juicy Info



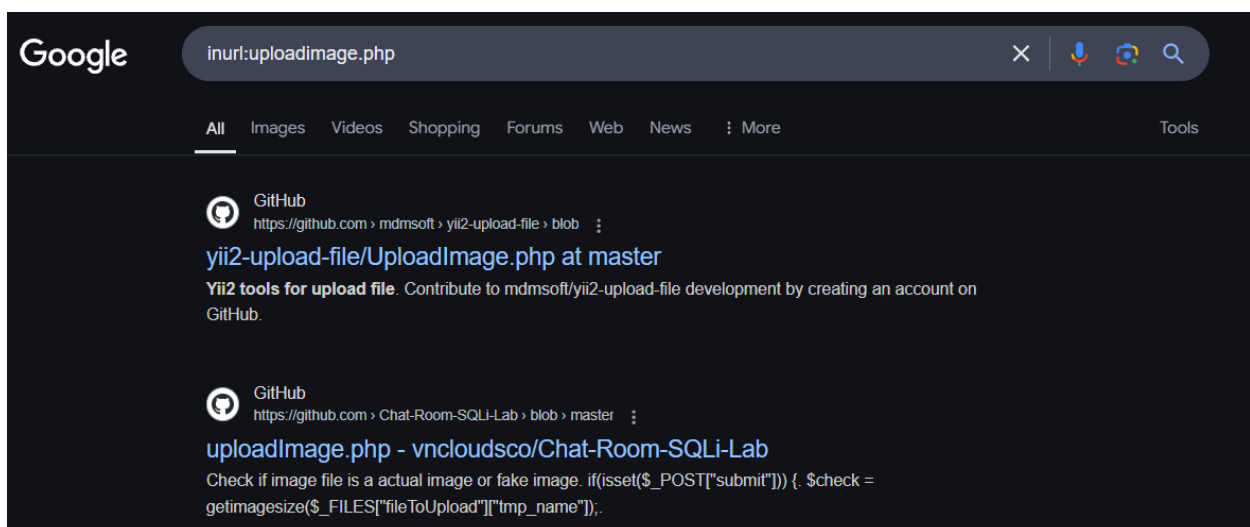
3) Various Online Devices



4) Sensitive Directories



5) Vulnerable Files



C. Write a dork for the following:**1. Log files for the login credentials**

filetype:log intext:"username" intext:"password"

2. Open FTP servers

intitle:"index of" "ftp"

3. Fetch the excel files containing list if emails

filetype:xls OR filetype:xlsx intext:"email"

4. List only pdf files from the any website

site:geeksforgeek.com filetype:pdf

5. View most recent Cache

cache:gtu.ac.in