

## **Module 3 OSINT Open source intelligence**

Task 1 sub domain find information using sublist3r

Task2 Find DNS Record for the domain

Using tools

- Dnsrecon /in built in kali linux

Task3 Find DNS record of particular domain

Using Dig / in built in kali linux

Task4 how to convert zone transfer

Using Dig

Task5 how to access live web camp using shodan

Task6 search for contact information email address and telephone number

Task7 identify key email address through harvester

Task8 find the details the old website

There was website archive.org

Task 9 How to enumerate key email address

There was website: I have been pwned

Task10 look for sensitive information in mail

There was website mx toolbox

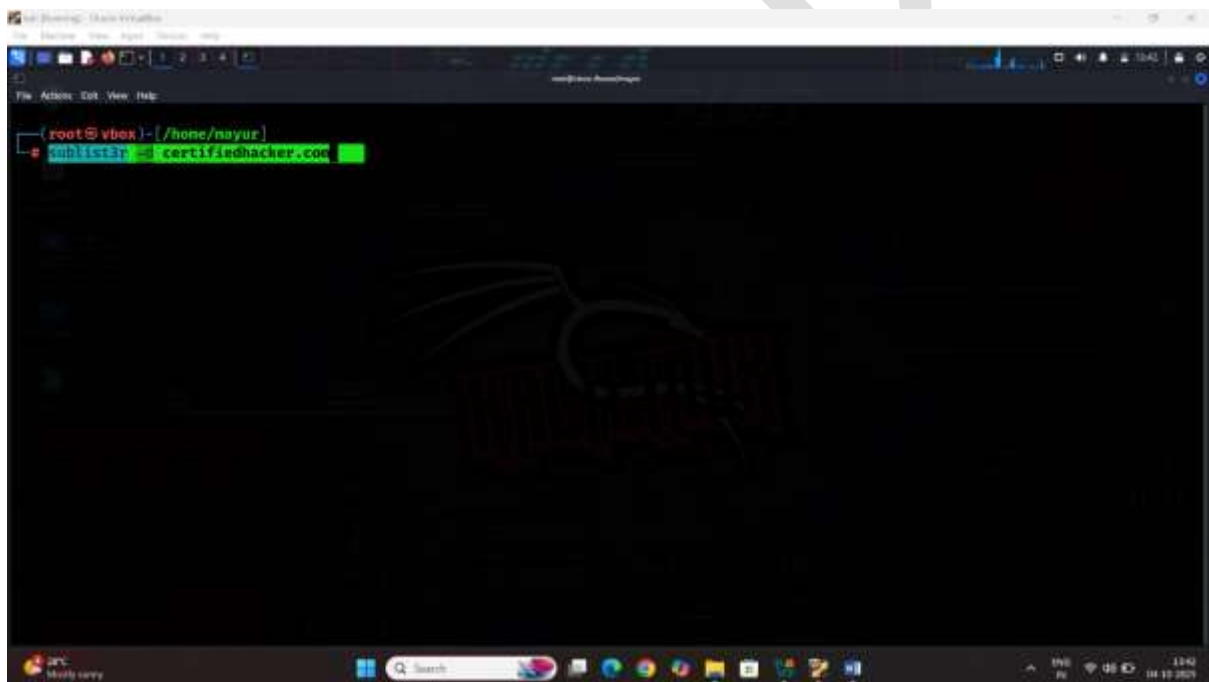
Task11 Evaluate osint automation tools using maltego

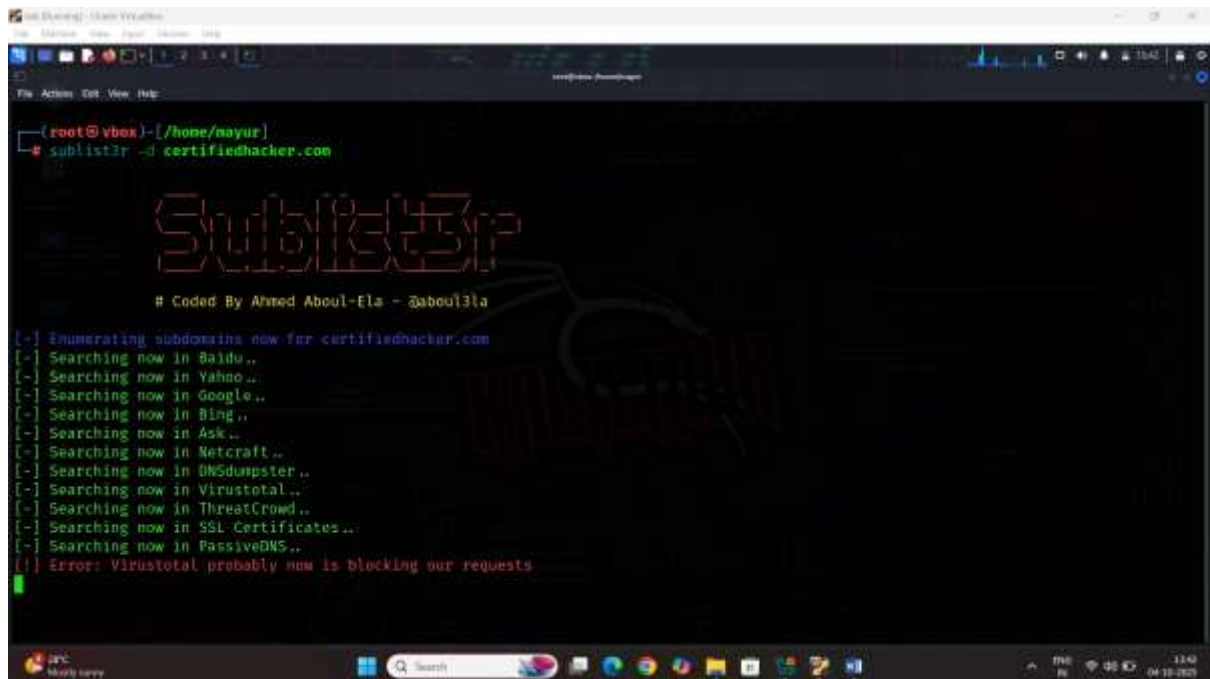
MAYUR

## Task 1 sub domain find information using sublist3r

Step1 start the kali Linux machine

Command: `sublist3r -d certifiedhacker.com`





```

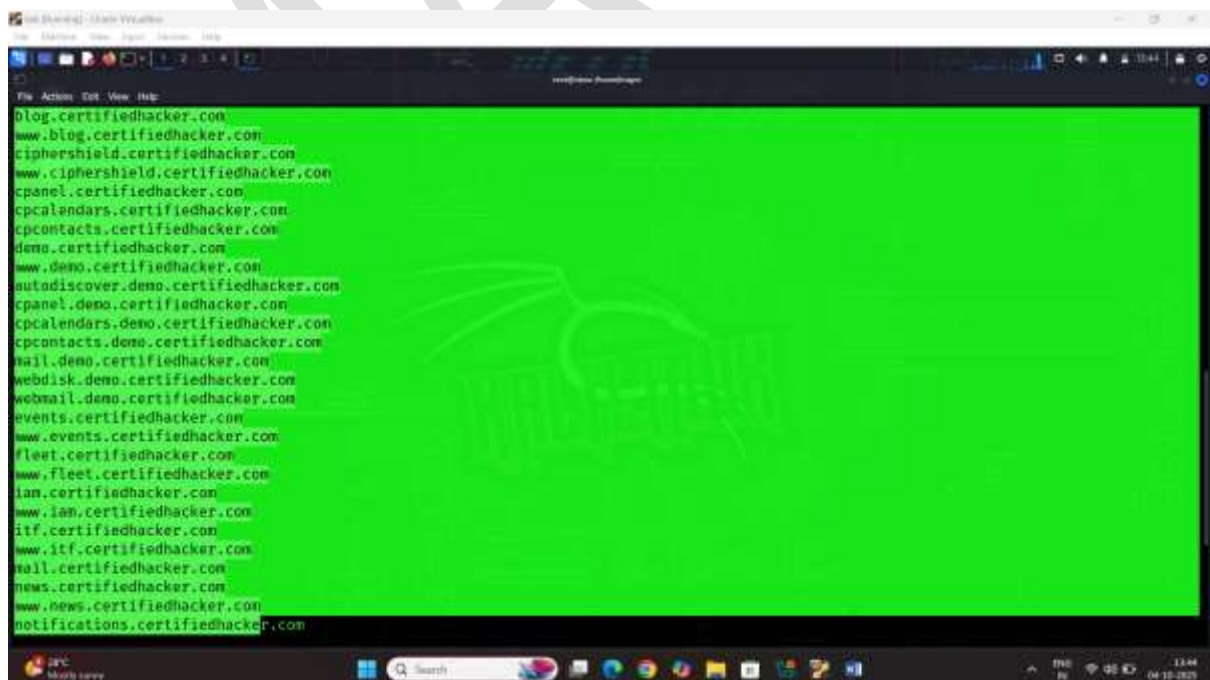
root@vbox: ~/hone/nayur
# sublist3r -d certifiedhacker.com

SUBLIST3R

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for certifiedhacker.com
[-] Searching now in Baldu..
[-] 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
  
```

## Result



```

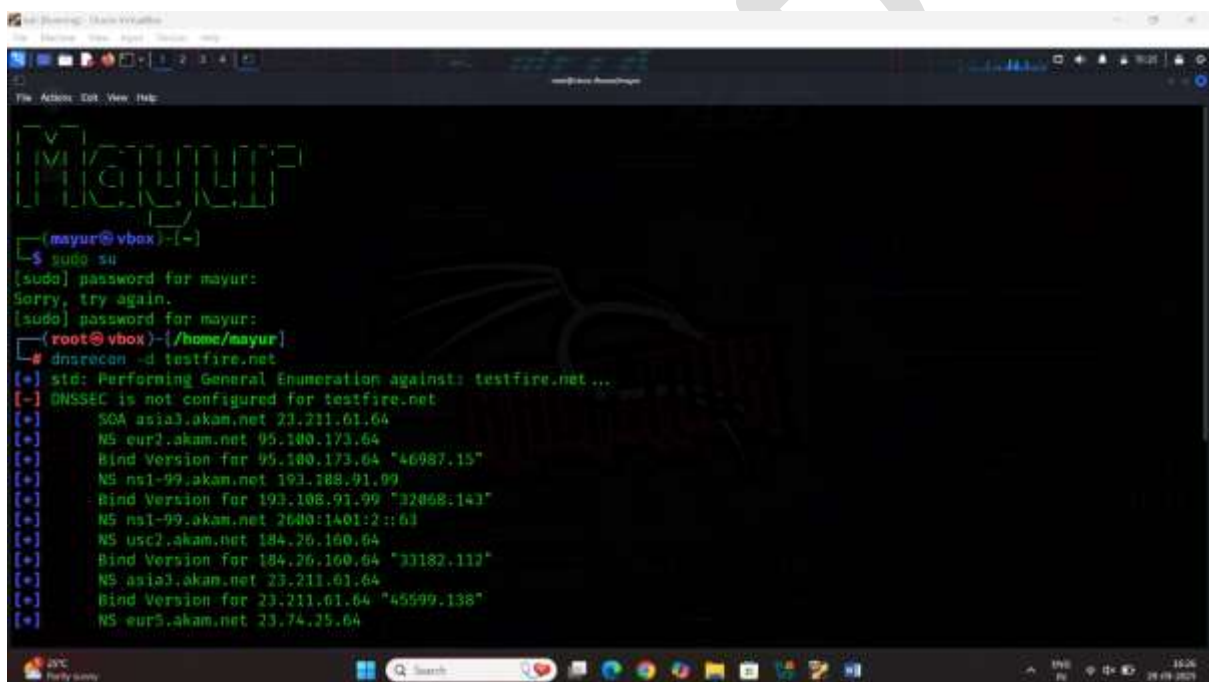
blog.certifiedhacker.com
www.blog.certifiedhacker.com
ciphershield.certifiedhacker.com
www.ciphershield.certifiedhacker.com
cpanel.certifiedhacker.com
cpanelendars.certifiedhacker.com
cpcontacts.certifiedhacker.com
demo.certifiedhacker.com
www.demo.certifiedhacker.com
autodiscover.demo.certifiedhacker.com
cpanel.demo.certifiedhacker.com
cpanelendars.demo.certifiedhacker.com
cpcontacts.demo.certifiedhacker.com
mail.demo.certifiedhacker.com
webdisk.demo.certifiedhacker.com
webmail.demo.certifiedhacker.com
events.certifiedhacker.com
www.events.certifiedhacker.com
fleet.certifiedhacker.com
www.fleet.certifiedhacker.com
lan.certifiedhacker.com
www.lan.certifiedhacker.com
itf.certifiedhacker.com
www.itf.certifiedhacker.com
mail.certifiedhacker.com
news.certifiedhacker.com
www.news.certifiedhacker.com
notifications.certifiedhacker.com
  
```

## Task2 Find DNS Record for the domain

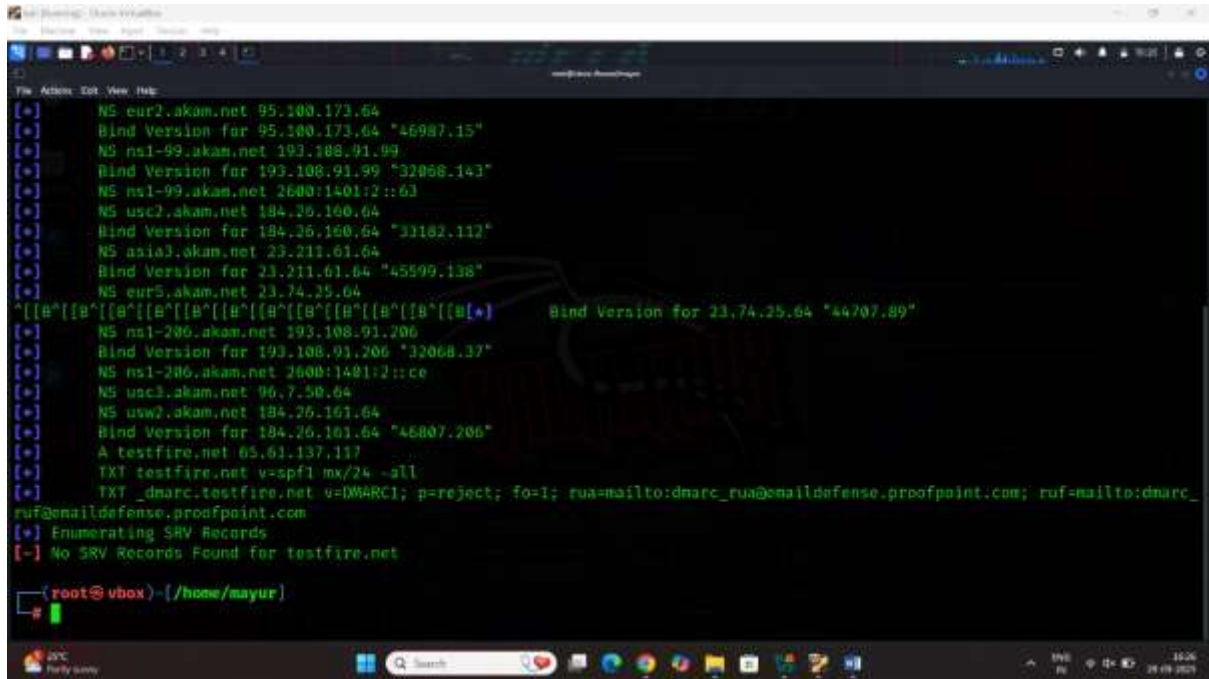
Step1 start the kali linux

Type the command: `dnsrecon -d testfire.net`

Result:



```
(mayur@vbox)~$ sudo su
[sudo] password for mayur:
[sudo] password for mayur:
(mayur@vbox)~$ dnsrecon -d testfire.net
[*] std: Performing General Enumeration against: testfire.net ...
[-] DNSSEC is not configured for testfire.net
[*] SOA asia3.akam.net 23.211.61.64
[*] NS eur2.akam.net 95.100.173.64
[*] Bind Version for 95.100.173.64 "46987.15"
[*] NS ns1-99.akam.net 193.108.91.09
[*] Bind Version for 193.108.91.09 "32068.143"
[*] NS ns1-99.akam.net 2600:1401:2::61
[*] NS usc2.akam.net 184.26.160.64
[*] Bind Version for 184.26.160.64 "33182.117"
[*] NS asia3.akam.net 23.211.61.64
[*] Bind Version for 23.211.61.64 "45599.138"
[*] NS eur5.akam.net 23.74.25.64
```



```

[*] NS eur2.akam.net 95.100.173.64
[*] Bind Version for 95.100.173.64 "46987.15"
[*] NS ns1-99.akam.net 193.108.91.99
[*] Bind Version for 193.108.91.99 "32068.143"
[*] NS ns1-99.akam.net 2600:1401:2::63
[*] NS usci2.akam.net 184.26.160.64
[*] Bind Version for 184.26.160.64 "33182.112"
[*] NS asia3.akam.net 23.211.61.64
[*] Bind Version for 23.211.61.64 "45599.138"
[*] NS eur5.akam.net 23.74.25.64
[*] Bind Version for 23.74.25.64 "44707.89"
[*] NS ns1-206.akam.net 193.108.91.206
[*] Bind Version for 193.108.91.206 "32068.137"
[*] NS ns1-206.akam.net 2600:1401:2::ce
[*] NS usci3.akam.net 96.7.50.64
[*] NS usw2.akam.net 184.26.161.64
[*] Bind Version for 184.26.161.64 "46807.206"
[*] A testfire.net 65.61.137.117
[*] TXT testfire.net v=spf1 mx/24 -all
[*] TXT _dmarc.testfire.net v=DMARC1; p=reject; fo=1; rua=mailto:dnarc_rua@emaildefense.proofpoint.com; ruf=mailto:dnarc_ruf@emaildefense.proofpoint.com
[*] Enumerating SRV Records
[-] No SRV Records Found for testfire.net

(root@ vbox) - (/home/mayur)

```

## Task3 Find DNS record of particular domain

Step1 start the kali linux

Type the command Dig ns testfire.net

Result:

```

(root@vbox)-[/home/mayur]
# dig ns testfire.net
;; communications error to 192.168.1.1453: timed out

<<>> DiG 9.20.2-1-Debian <<>> ns testfire.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 37523
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;testfire.net.                IN      NS

;; ANSWER SECTION:
testfire.net.                21600   IN      NS      usw2.akam.net.
testfire.net.                21600   IN      NS      ns1-99.akam.net.
testfire.net.                21600   IN      NS      usc3.akam.net.
testfire.net.                21600   IN      NS      eur2.akam.net.
testfire.net.                21600   IN      NS      eur5.akam.net.
testfire.net.                21600   IN      NS      ns1-206.akam.net.
testfire.net.                21600   IN      NS      usc2.akam.net.
testfire.net.                21600   IN      NS      asia3.akam.net.

;; Query time: 3653 msec
;; SERVER: 192.168.1.1453(192.168.1.1) (UDP)
;; WHEN: Mon Sep 29 16:27:00 IST 2025
;; MSG SIZE rcvd: 284

(root@vbox)-[/home/mayur]

```

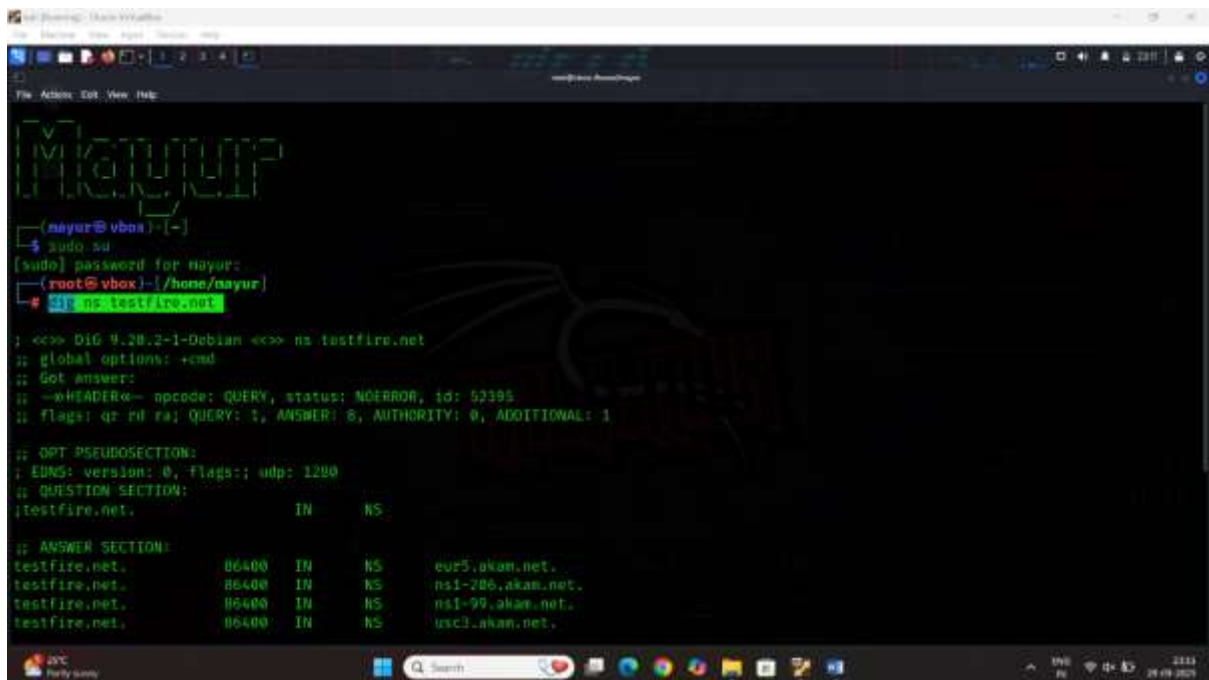
## Task4 how to convert zone transfer

### Using Dig

Step1 start the kali linux

Step2 find the dns record of the domain

## Command dig ns testfire.net



```

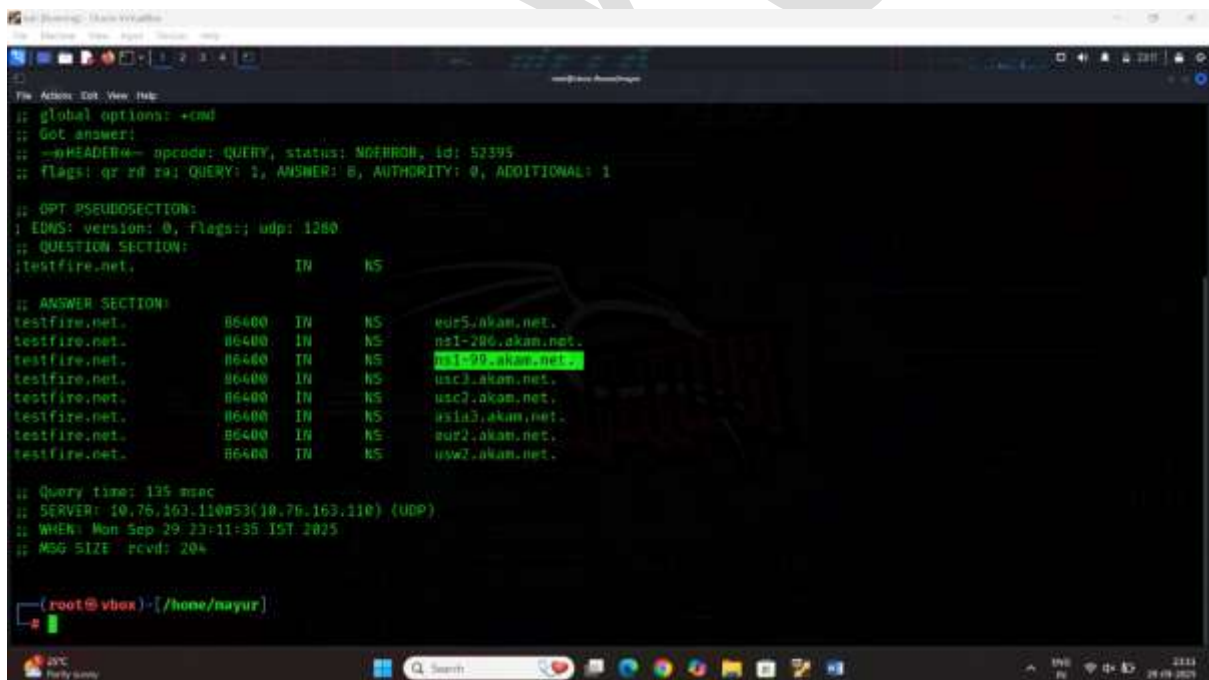
(mayur@vbox)~$ sudo su
[sudo] password for mayur:
(root@vbox)~$ dig ns testfire.net

<<>> DIG 9.20.2-1-Debian <<>> ns testfire.net
;; global options: +cmd
;; Got answer:
;;->HEADER<- opcode: QUERY, status: NOERROR, id: 52395
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;testfire.net.                IN      NS

;; ANSWER SECTION:
testfire.net.                86400   IN      NS      eur5.akam.net.
testfire.net.                86400   IN      NS      ns1-286.akam.net.
testfire.net.                86400   IN      NS      ns1-99.akam.net.
testfire.net.                86400   IN      NS      usc3.akam.net.

```



```

(root@vbox)~$ dig @ns1-99.akam.net testfire.net axfr

;; global options: +cmd
;; Got answer:
;;->HEADER<- opcode: QUERY, status: NOERROR, id: 52395
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;testfire.net.                IN      NS

;; ANSWER SECTION:
testfire.net.                86400   IN      NS      eur5.akam.net.
testfire.net.                86400   IN      NS      ns1-286.akam.net.
testfire.net.                86400   IN      NS      ns1-99.akam.net.
testfire.net.                86400   IN      NS      usc3.akam.net.
testfire.net.                86400   IN      NS      usc2.akam.net.
testfire.net.                86400   IN      NS      asia3.akam.net.
testfire.net.                86400   IN      NS      eur2.akam.net.
testfire.net.                86400   IN      NS      usw2.akam.net.

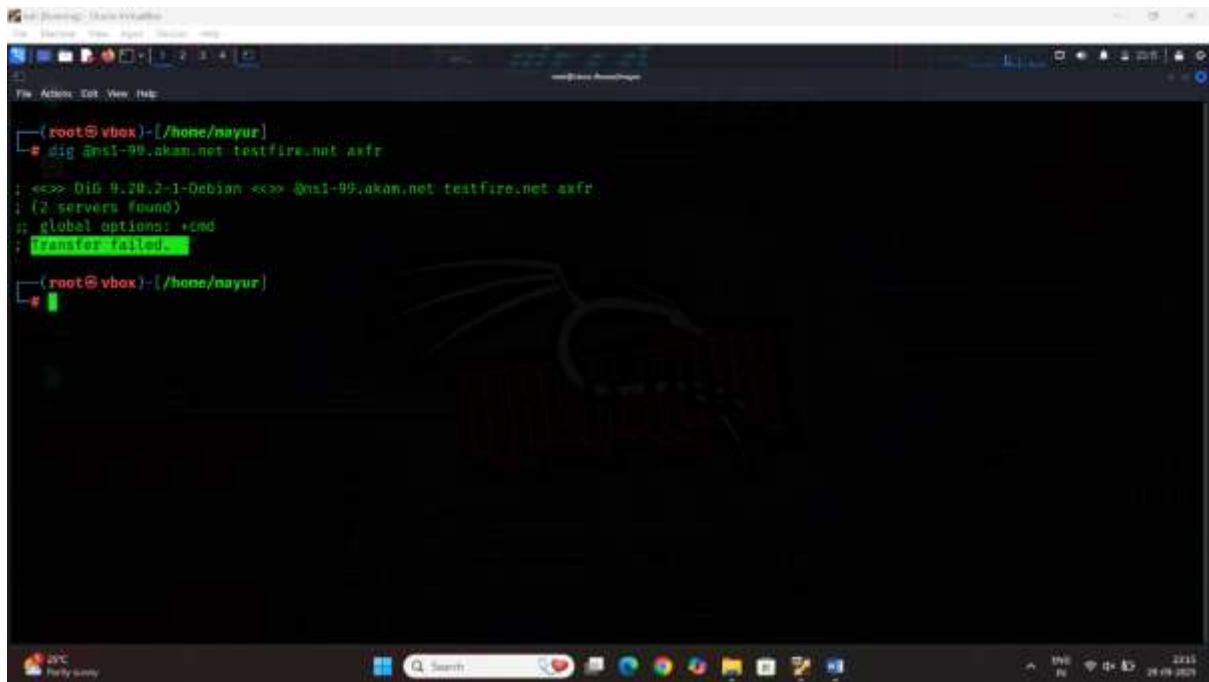
;; Query time: 125 msec
;; SERVER: 10.76.163.110#53(10.76.163.110) (UDP)
;; WHEN: Mon Sep 29 23:11:35 IST 2025
;; MSG SIZE  rcvd: 204

```

Step3 copy the dns recode

Command dig @ns1-99.akm.net testfire.net axfr

Result:



```

(root@vbox)-[/home/nayur]
# dig @ns1-99.akan.net testfire.net axfr

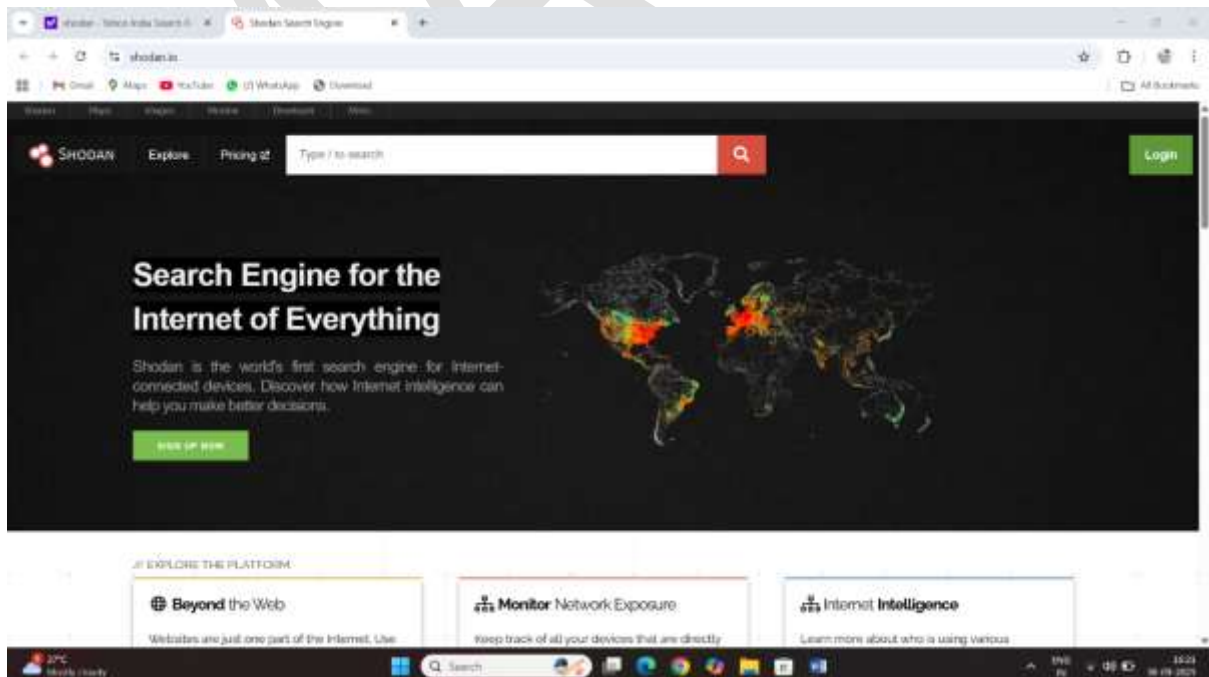
<>> 9.20.2-1-Debian <>> @ns1-99.akan.net testfire.net axfr
(2 servers found)
: global options: +end
: Transfer failed.

(root@vbox)-[/home/nayur]
#

```

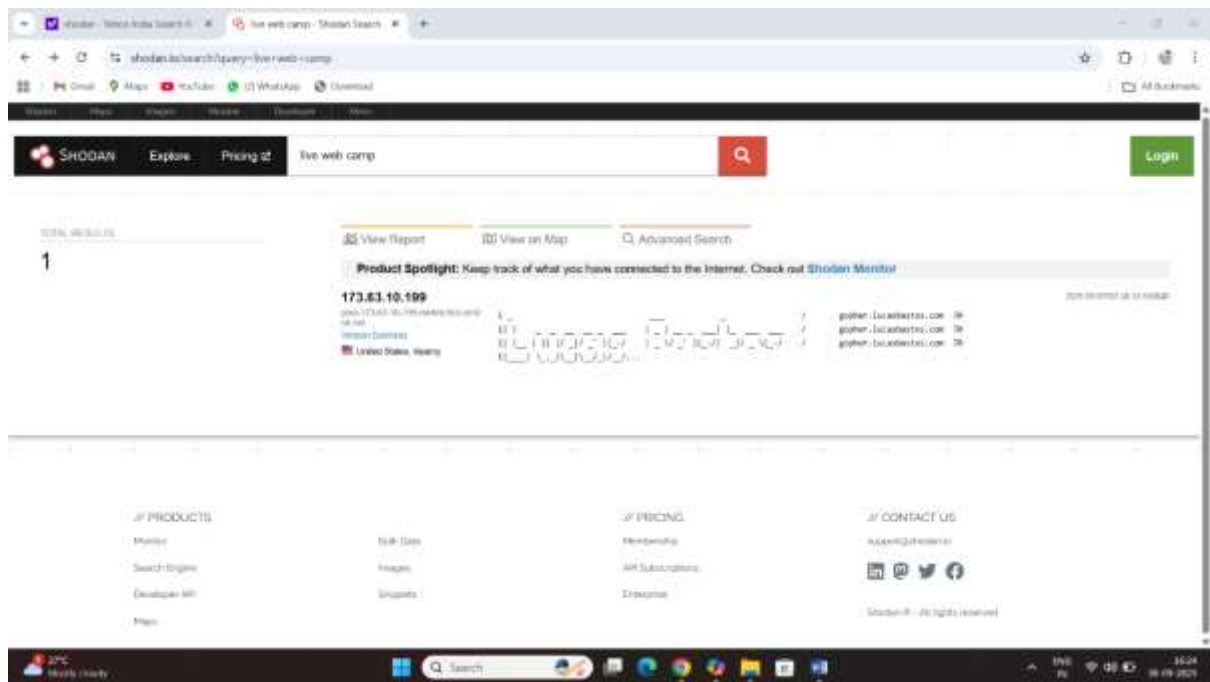
## Task5 how to access live web camp using shodan

Step1 open shodan engine

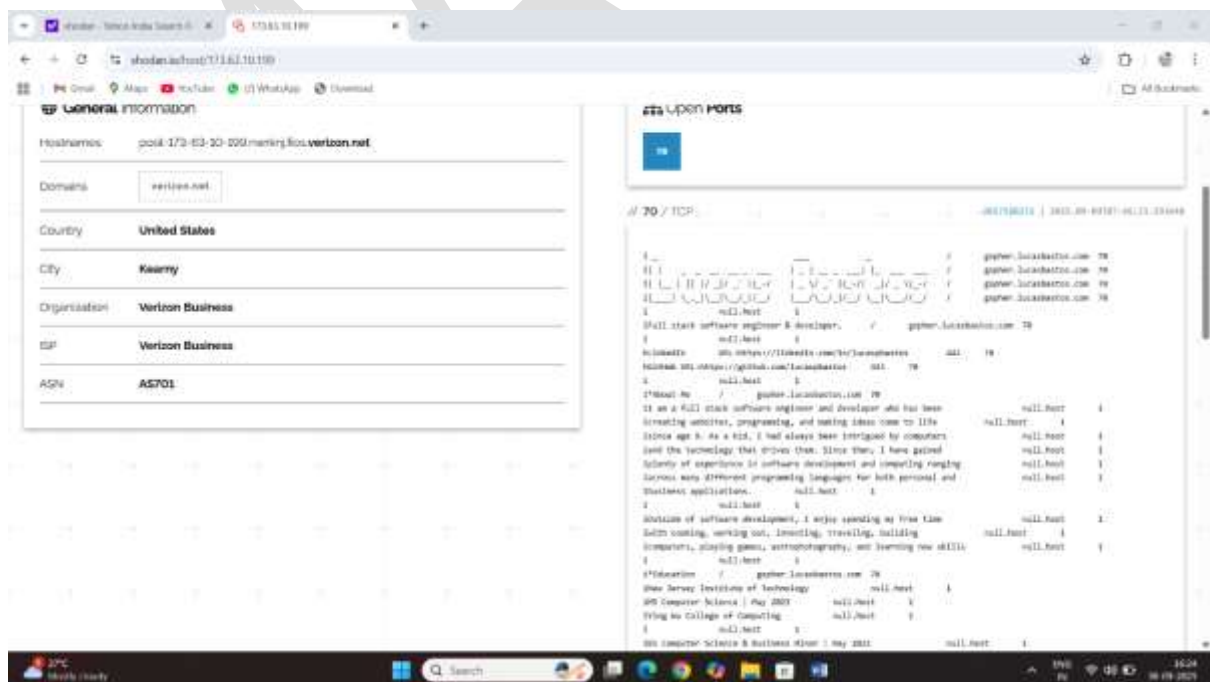


Step1 open the browser search the shodan

## Step2 search the camera

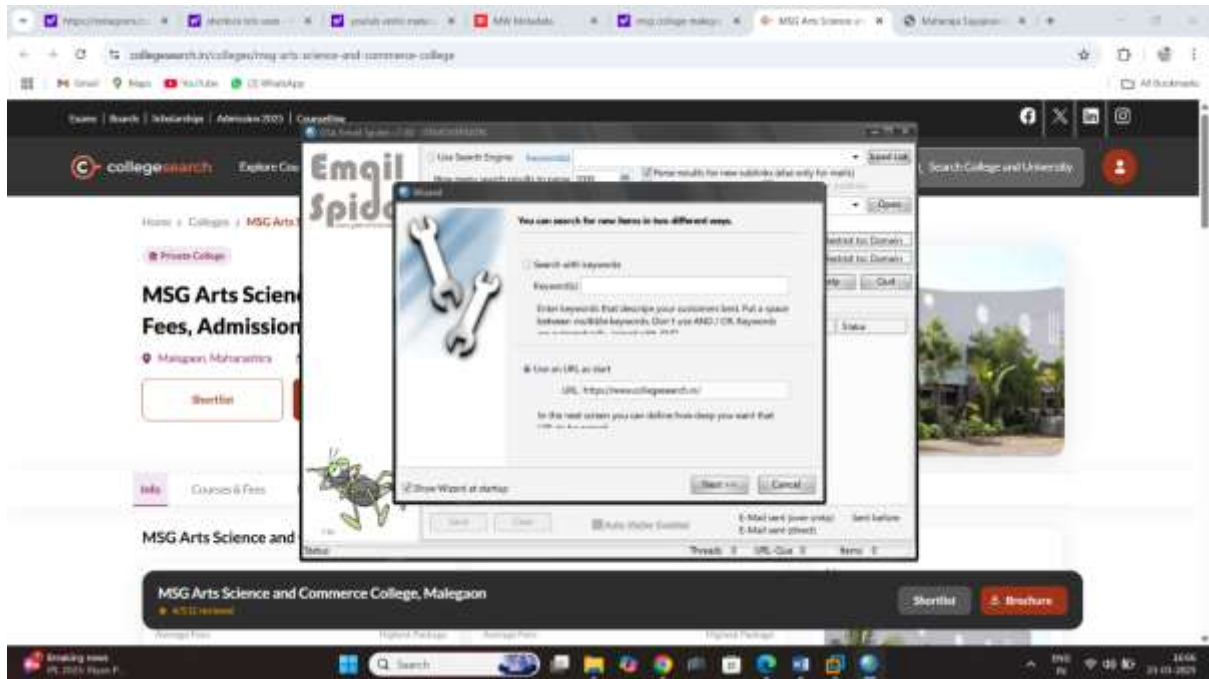


**Result:**



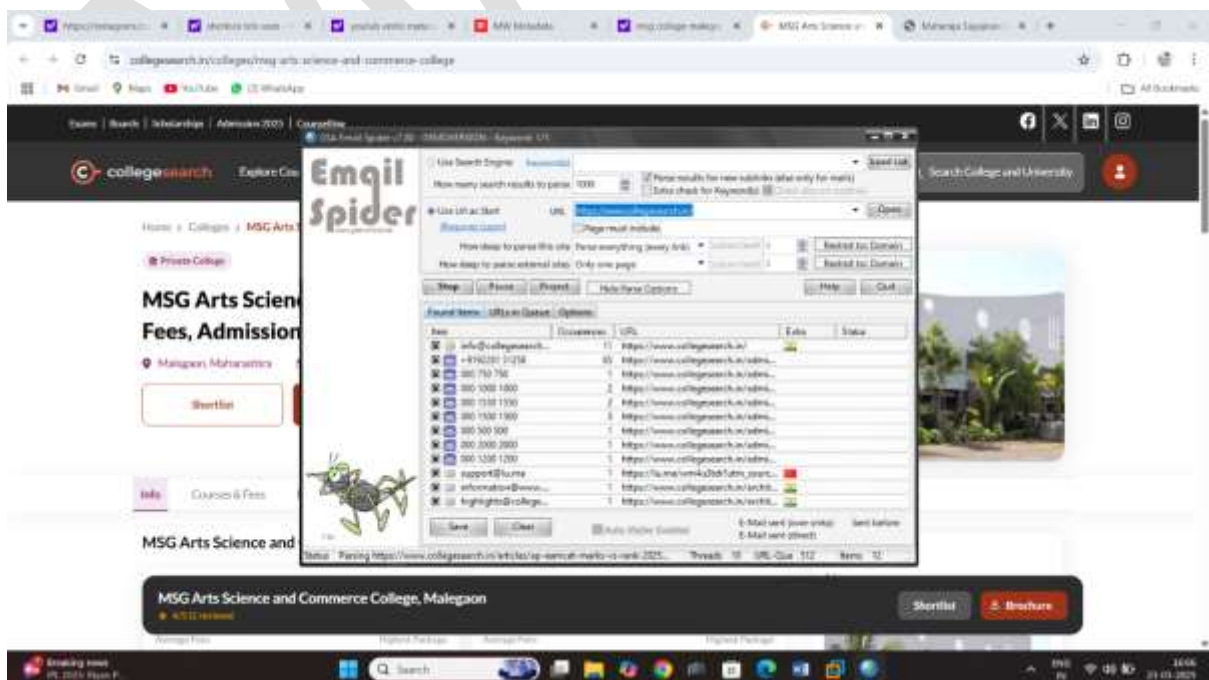
# Task6 serach for contact information email address and telephone number

Step1 start the email spider



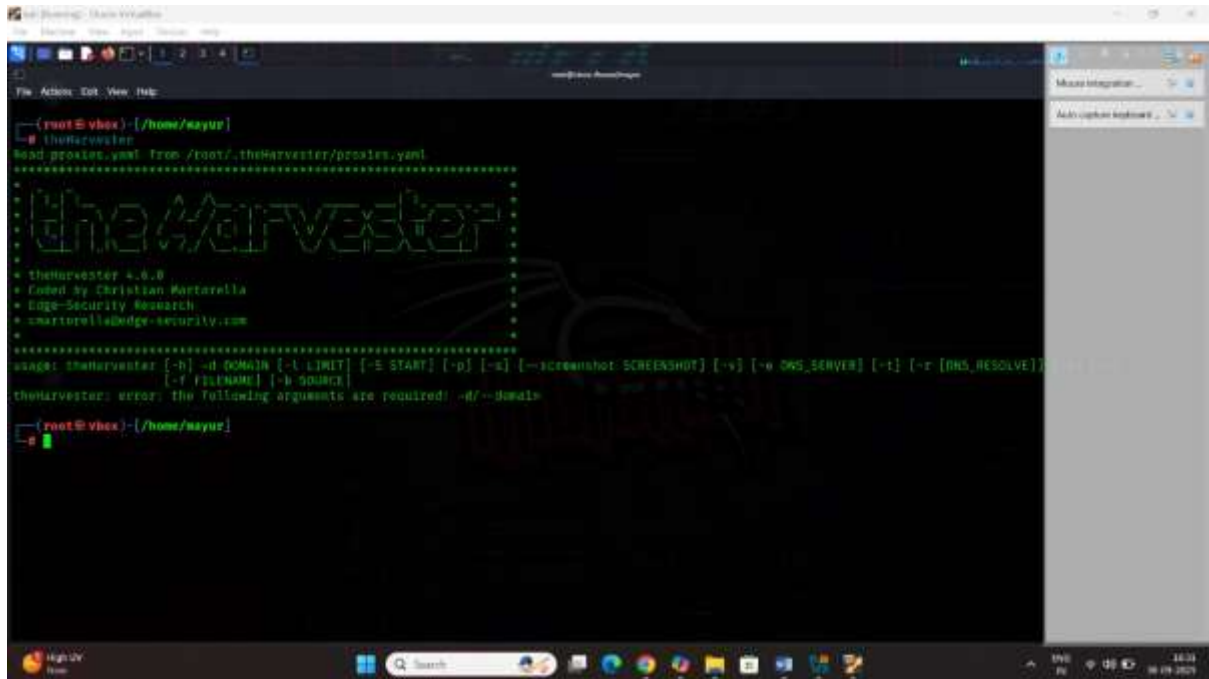
Step2 type the url certifiedhacker.com

Result:



# Task7 identify key email address through harvester

Step1 start the kali linux

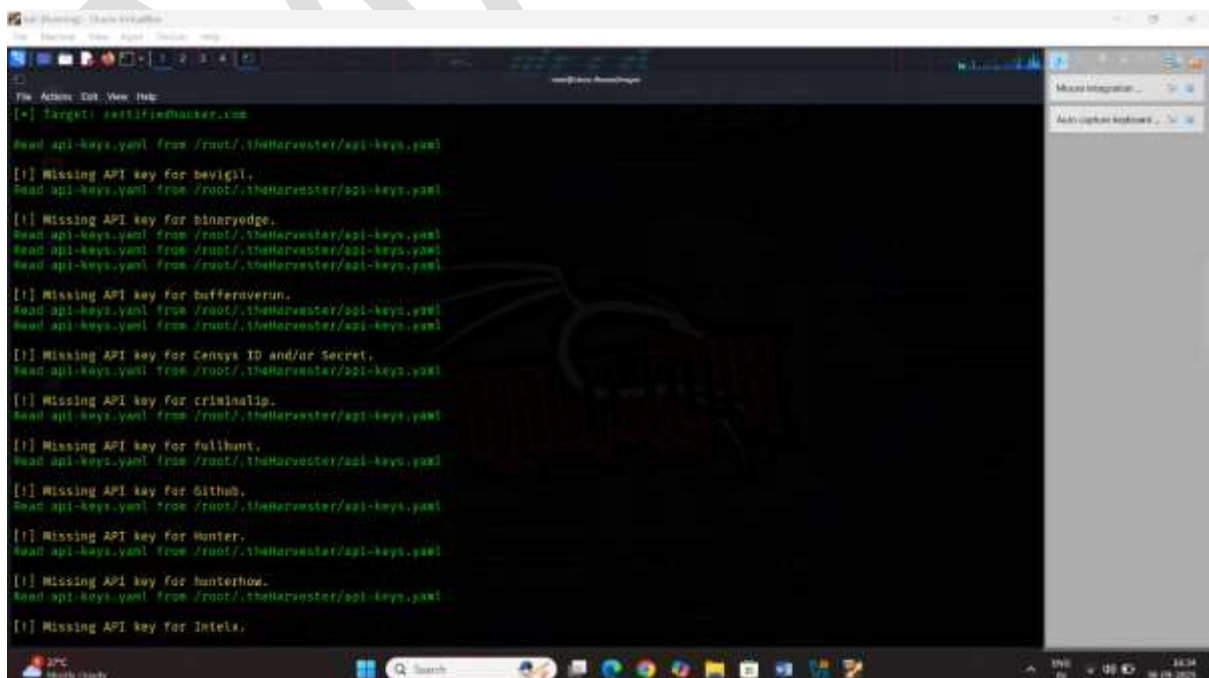


```

(root@vbox) ~/home/kayur
# theHarvester
Read proxies.yaml from /root/.theHarvester/proxies.yaml
*****
theHarvester
*****
theHarvester 4.6.8
* Created by Christian Martorella
* Edge-Security Research
* smarton@edge-security.com
*****
usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-s START] [-p] [-a] [--screenshot SCREENSHOT] [-v] [-w DNS_SERVER] [-t] [-r [DNS_RESOLVE]] [-f FILENAME] [-b SOURCE]
theHarvester: error: the following arguments are required: -d/--domain

(root@vbox) ~/home/kayur
  
```

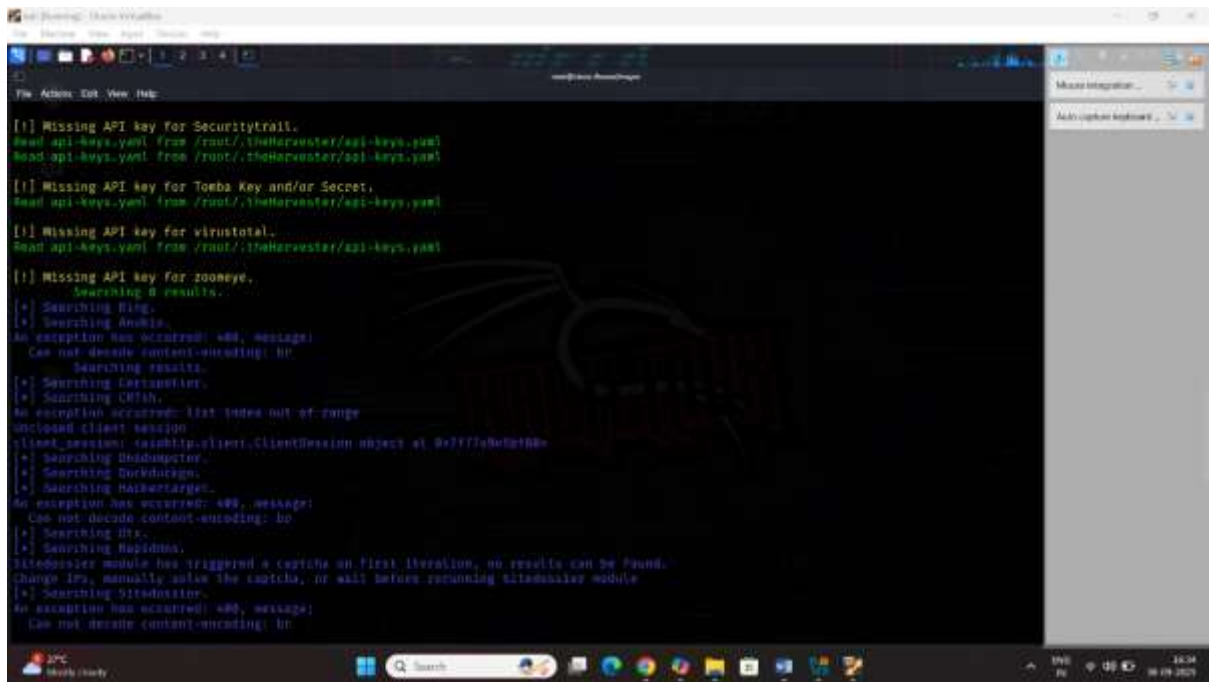
Using harvester/in built in kali



```

[*] Target: certifidhacker.com

Read api-keys.yaml from /root/.theHarvester/api-keys.yaml
[!] Missing API key for bevigil.
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml
[!] Missing API key for binaryedge.
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml
[!] Missing API key for bufferoverrun.
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml
[!] Missing API key for Censys ID and/or Secret.
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml
[!] Missing API key for criminalip.
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml
[!] Missing API key for fullhunt.
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml
[!] Missing API key for Github.
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml
[!] Missing API key for Hunter.
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml
[!] Missing API key for hunterio.
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml
[!] Missing API key for Intelx.
  
```



```
[!] Missing API key for Securitytrail.  
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml  
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml  
[!] Missing API key for Tombs Key and/or Secret.  
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml  
[!] Missing API key for VirusTotal.  
Read api-keys.yaml from /root/.theHarvester/api-keys.yaml  
[!] Missing API key for Zoomeye.  
Searching 0 results.  
[*] Searching Bing.  
[*] Searching Anubis.  
An exception has occurred: 400, message:  
Can not decode content-encoding: br  
Searching results.  
[*] Searching Certbot.  
[*] Searching CRTH.  
An exception has occurred: list index out of range  
upload client session  
client_session: <urllib3.client.ClientSession object at 0xffff9604b0b0>  
[*] Searching Outdamp.  
[*] Searching RockHopper.  
[*] Searching HackBar.  
An exception has occurred: 400, message:  
Can not decode content-encoding: br  
[*] Searching Hrs.  
[*] Searching RapidDNA.  
VirusTotal module has triggered a captcha on first iteration, no results can be found.  
Change IP, manually solve the captcha, or wait before re-running VirusTotal module  
[*] Searching VirusTotal.  
An exception has occurred: 400, message:  
Can not decode content-encoding: br
```

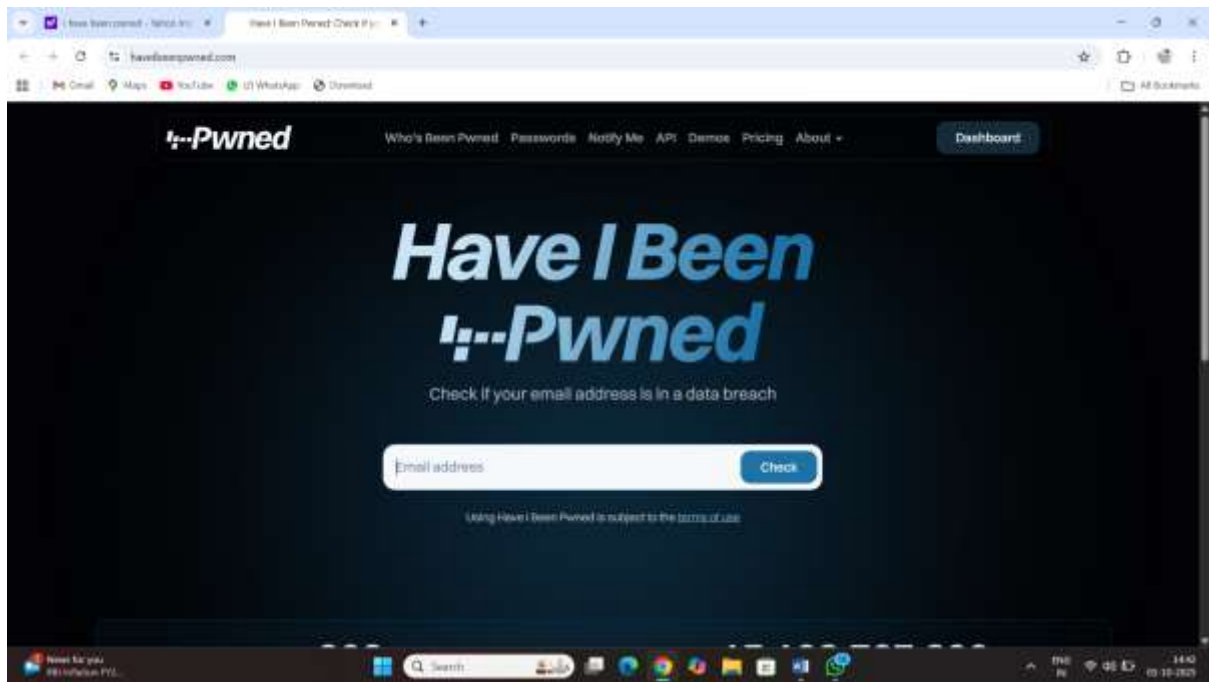
There was website archive.org



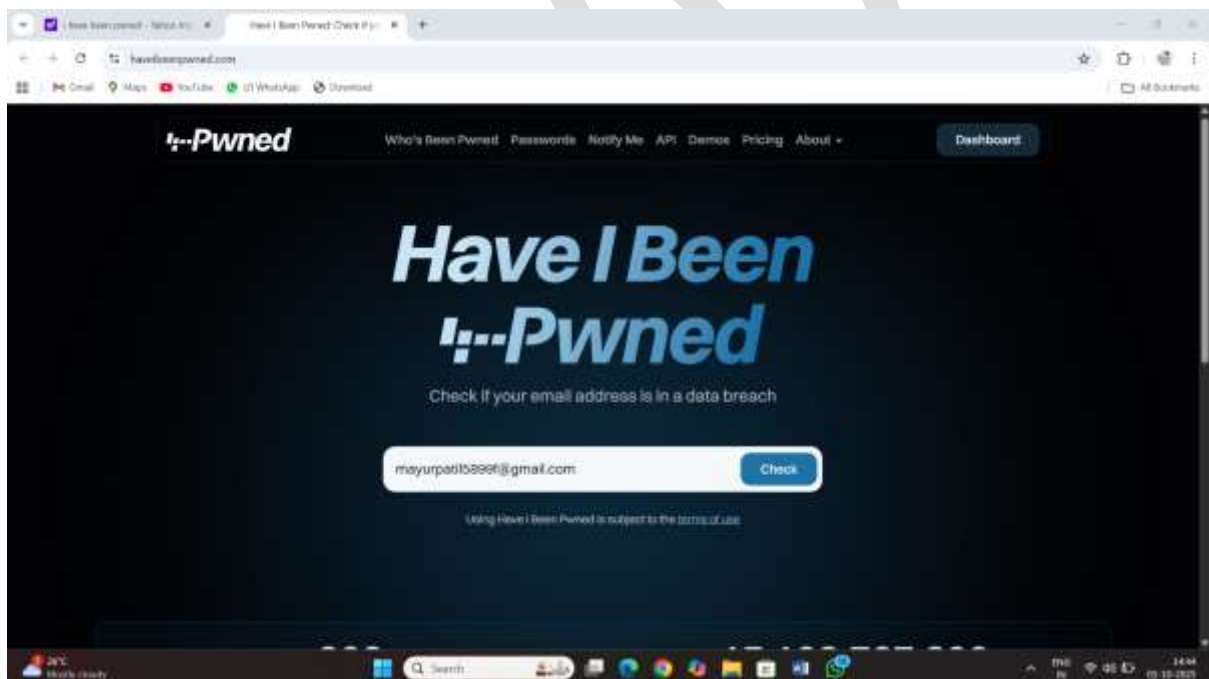
Step1 type the url domain



## Task 9 How to enumerate key email address

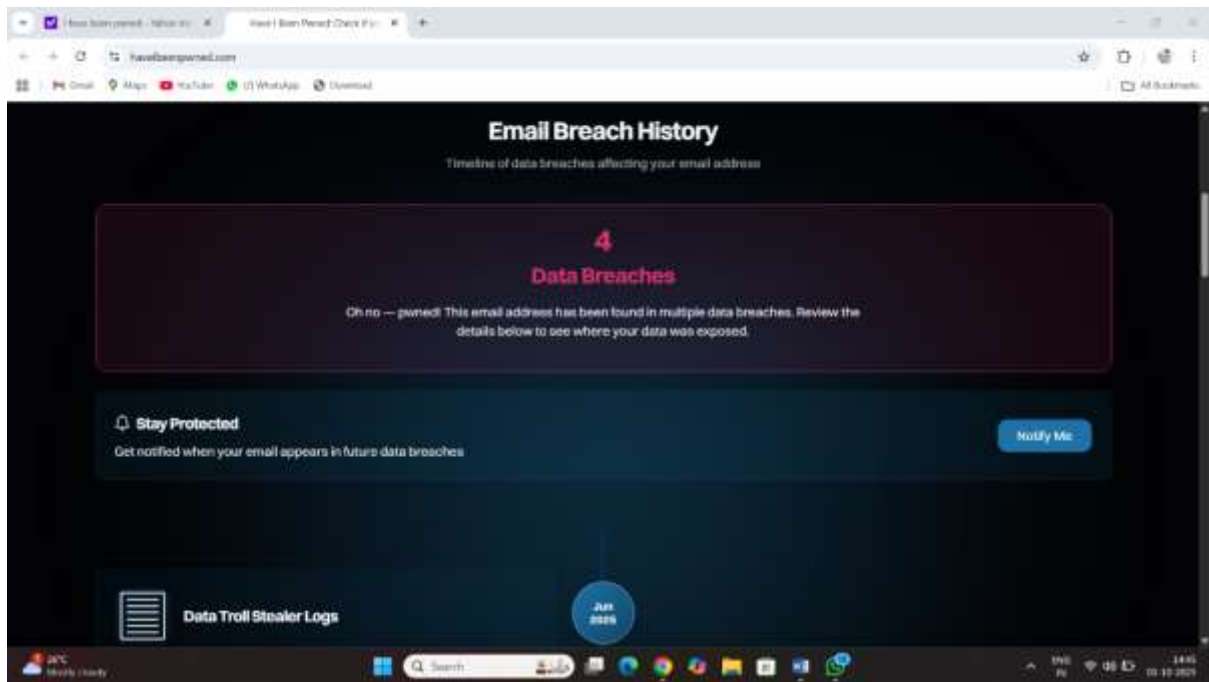


Step3 enter your email address



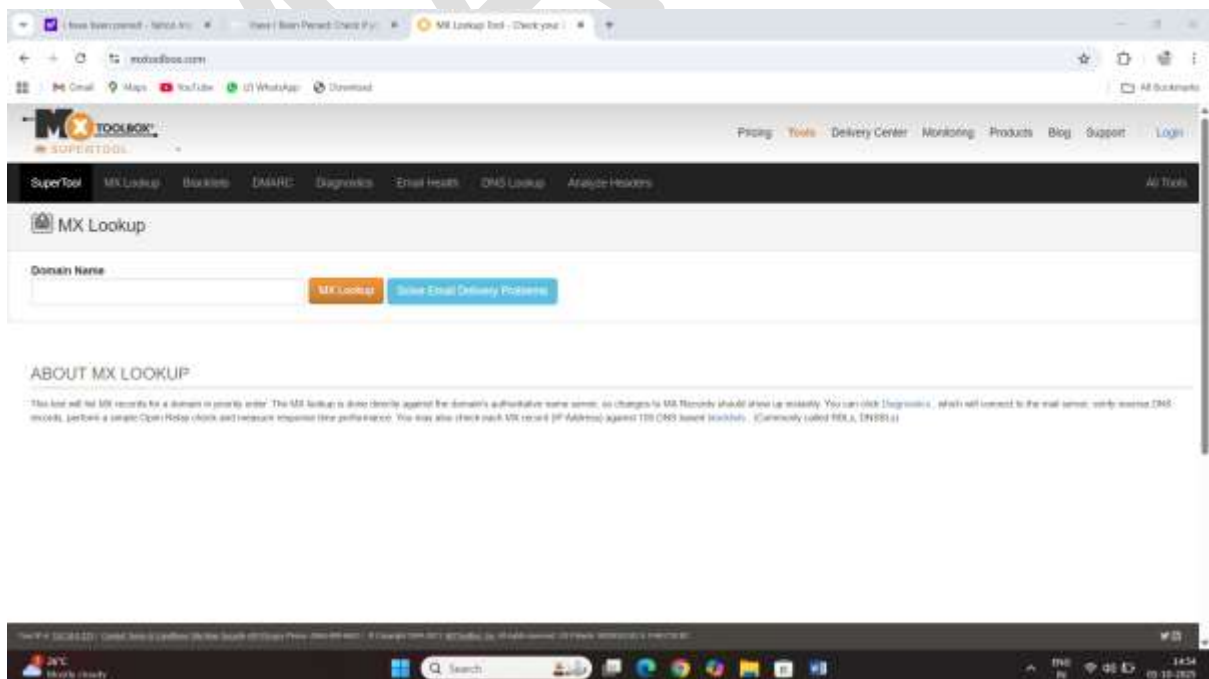
Step4 click on the check option

Result:



**Task10 look for sensitive information in mail**

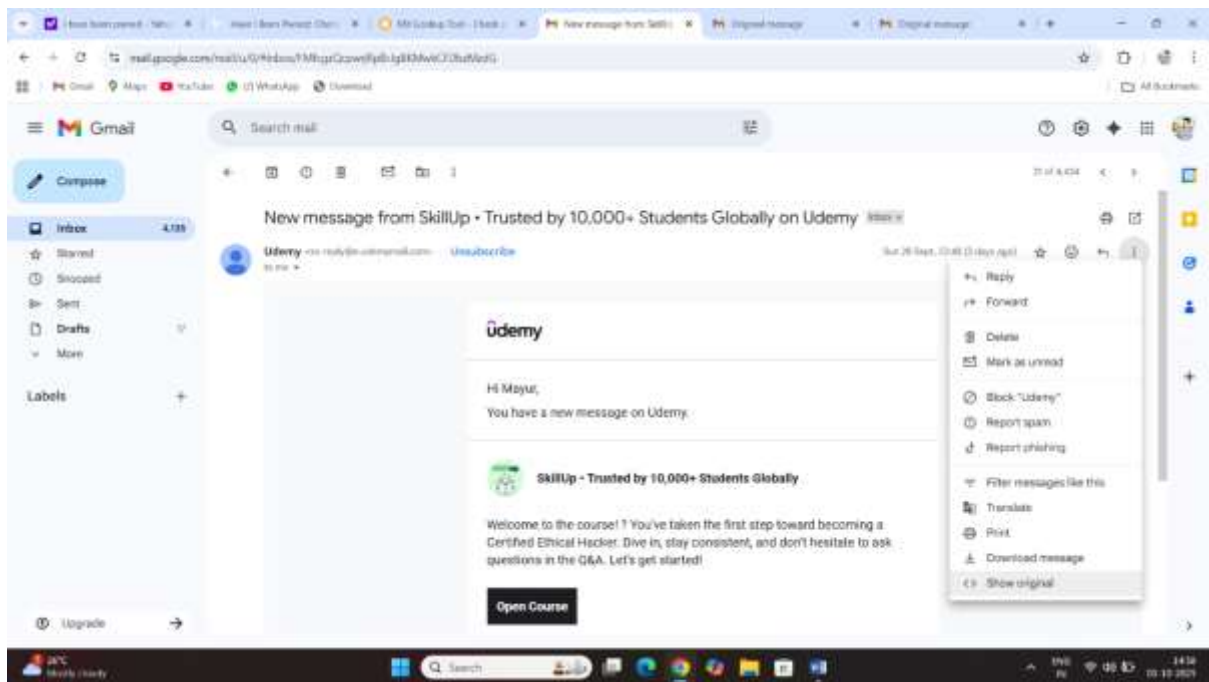
**There was website mx toolbox**



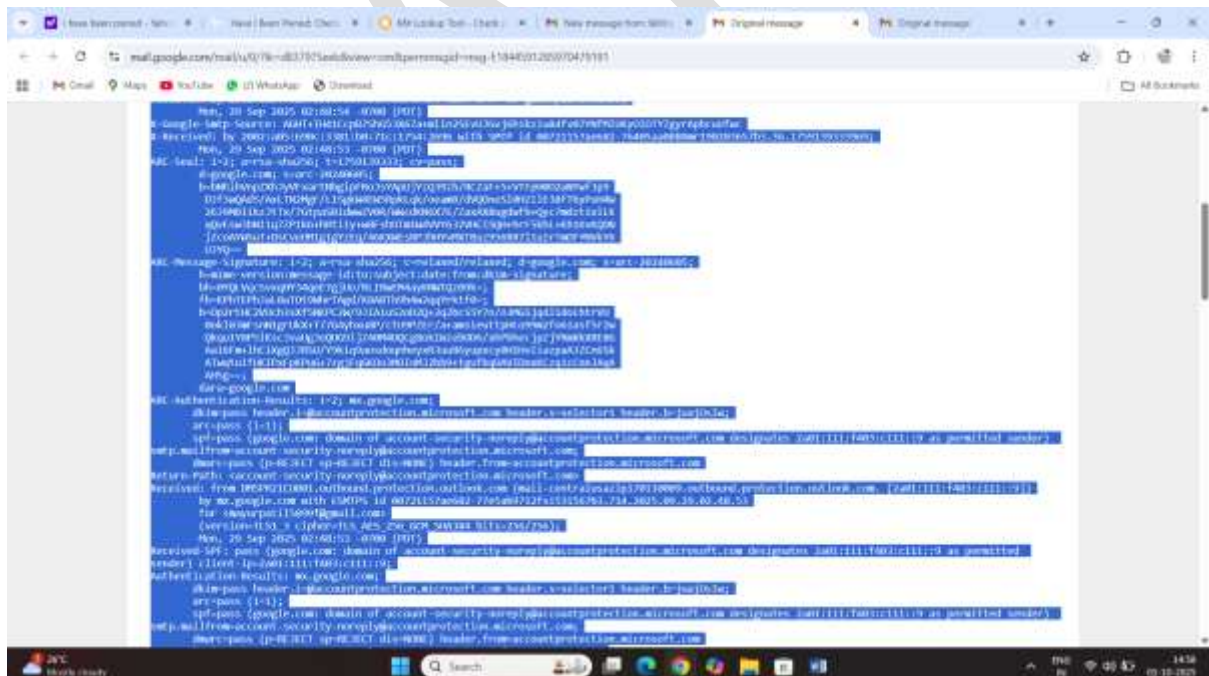
**Step2 select the email**

Step3 click on the email setting

Step4 show original option

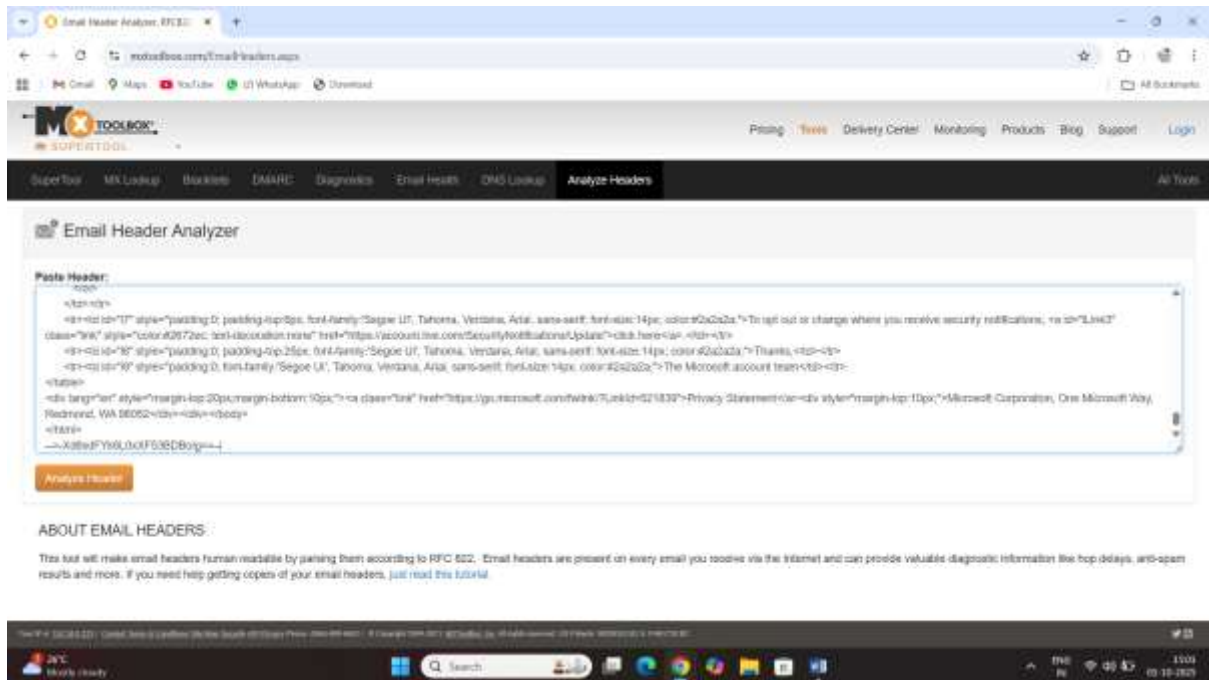


Step5 copy the email header



Step6 past the email header in toolbox

Step7 click on the headrs anaylis



## Result

The screenshot displays the Email Header Analyzer interface. The top section shows the email subject: "Microsoft account password change". Below this, the "Delivery Information" section lists several status checks, all of which are green, indicating they passed:

- DMARC Compliant
- SPF Alignment
- SPF Authenticated
- DKIM Alignment
- DKIM Authenticated

The "Relay Information" section shows the email was received in 8 seconds. Below this is a horizontal bar chart representing the relay path. The bottom section of the image shows a detailed table of the email's relay path, including the domain, IP address, and the server used for each hop.

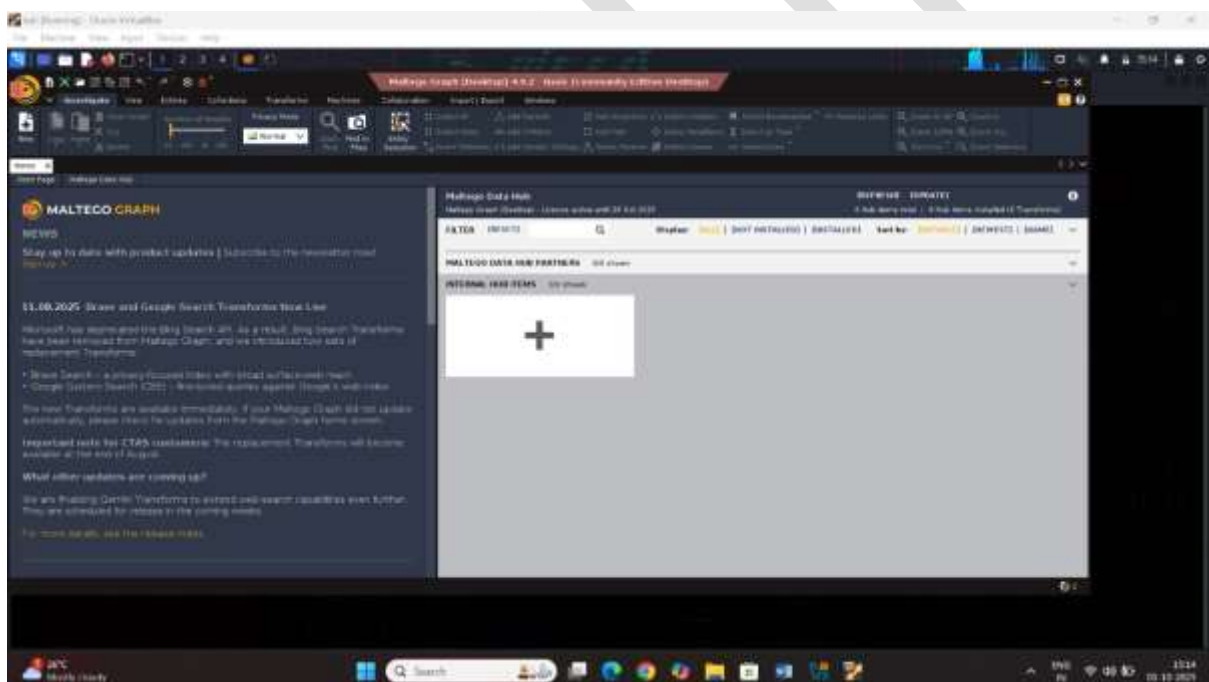
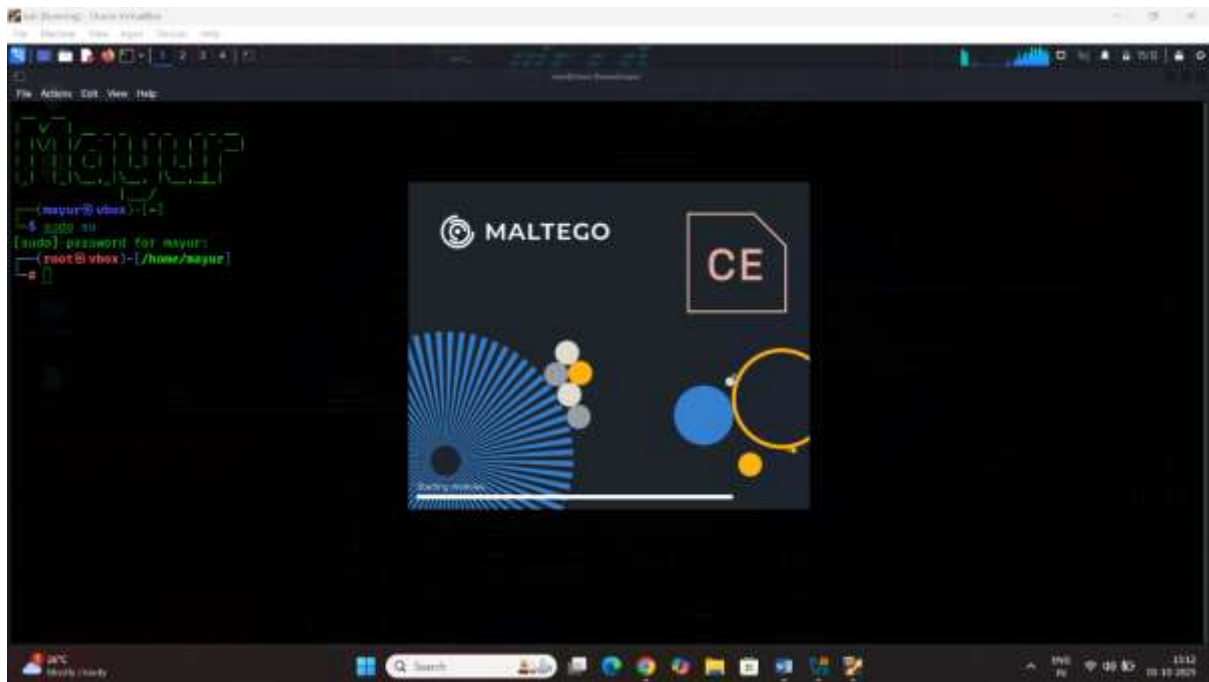
No.	Delay	From	By	With	Time (UTC)	Status
1	-	accountprotection.microsoft.com 23.48.229.238	5A2PEPT0003F02 mail.protection.outlook.com 10.10.7.243 37	Microsoft SMTP Server (version=TLSv1.3, cipher=TLS_AES_256_GCM_SHA384)	10/29/2025 9:40:52 AM	✓
2	0 seconds	5A2PEPT0003F02/smgpr014.prov.outlook.com 2003.180.0.0	5B6P020CA0016 outlook.office365.com 2003.180.0.0	Microsoft SMTP Server (version=TLSv1.3, cipher=TLS_AES_256_GCM_SHA384)	10/29/2025 9:40:56 AM	✓
3	-	5B6P020CA0016/prov.exchangelabs.com 2003.180.0.0	16.APR150033341/smgpr016.prov.outlook.com 2003.180.0.0	Microsoft SMTP Server (version=TLSv1.3, cipher=TLS_AES_256_GCM_SHA384)	10/29/2025 9:40:57 AM	✓
4	1 second	DMSPR2112J001/outbound.protection.outlook.com 2001.11.1.1803.111	msa.google.com	ESMTPS	10/29/2025 9:40:58 AM	✓
5	1 second	-	2002.402.11110.238c.93.43c.1587.9450	SMTP	10/29/2025 9:40:59 AM	✓

Below the table, there is a link: "Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center". The "SPF and DKIM Information" section shows the DMARC record for "dmarc:accountprotection.microsoft.com" and a "Show" button. Below this is a green box containing the DMARC record details.

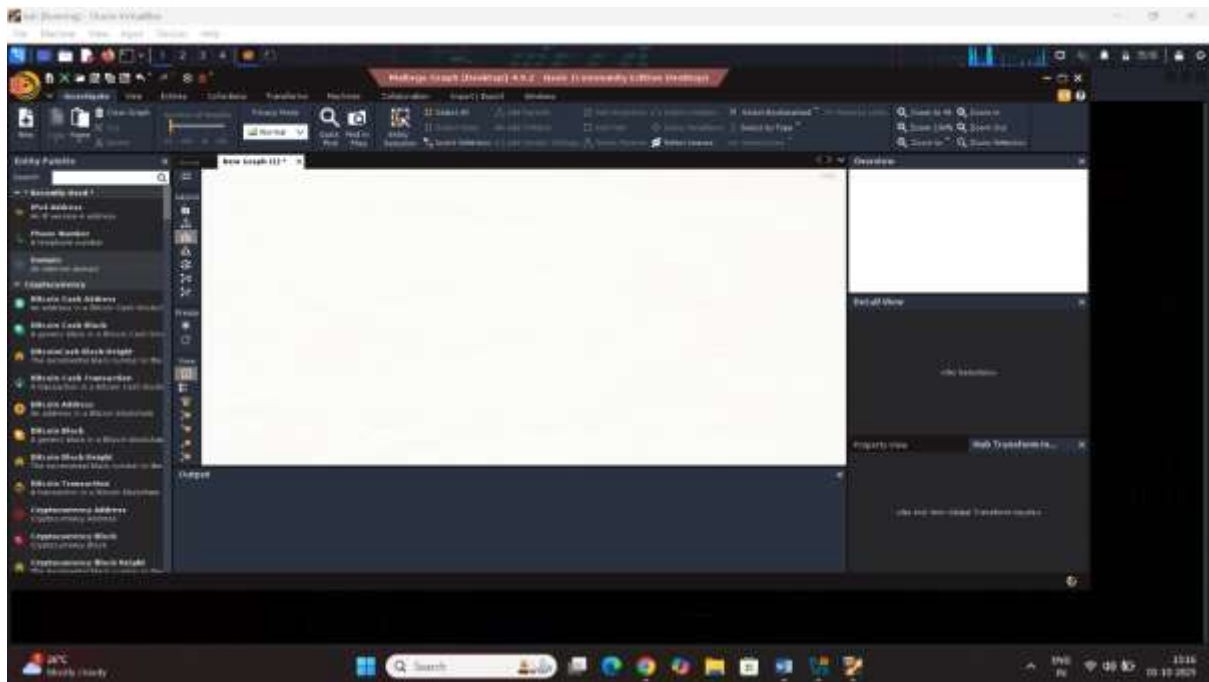
## Task11 Evaluate osint automation tools

Step1 open the kali linux machine

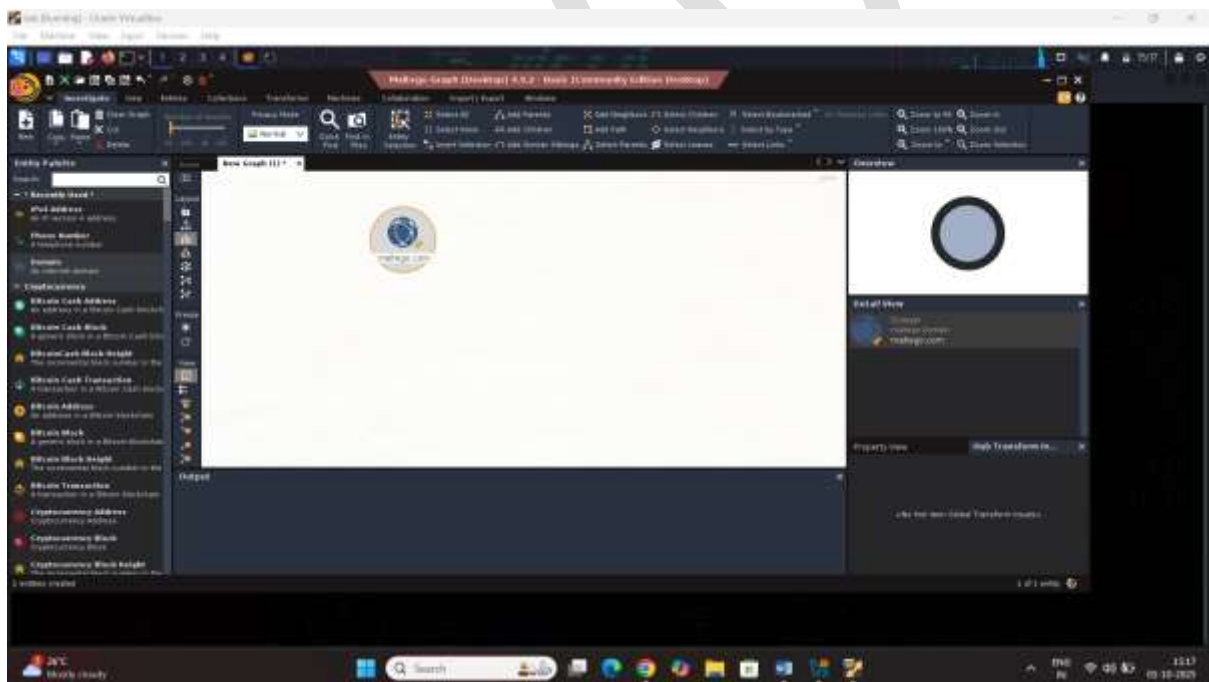
Step2 start the malego tool



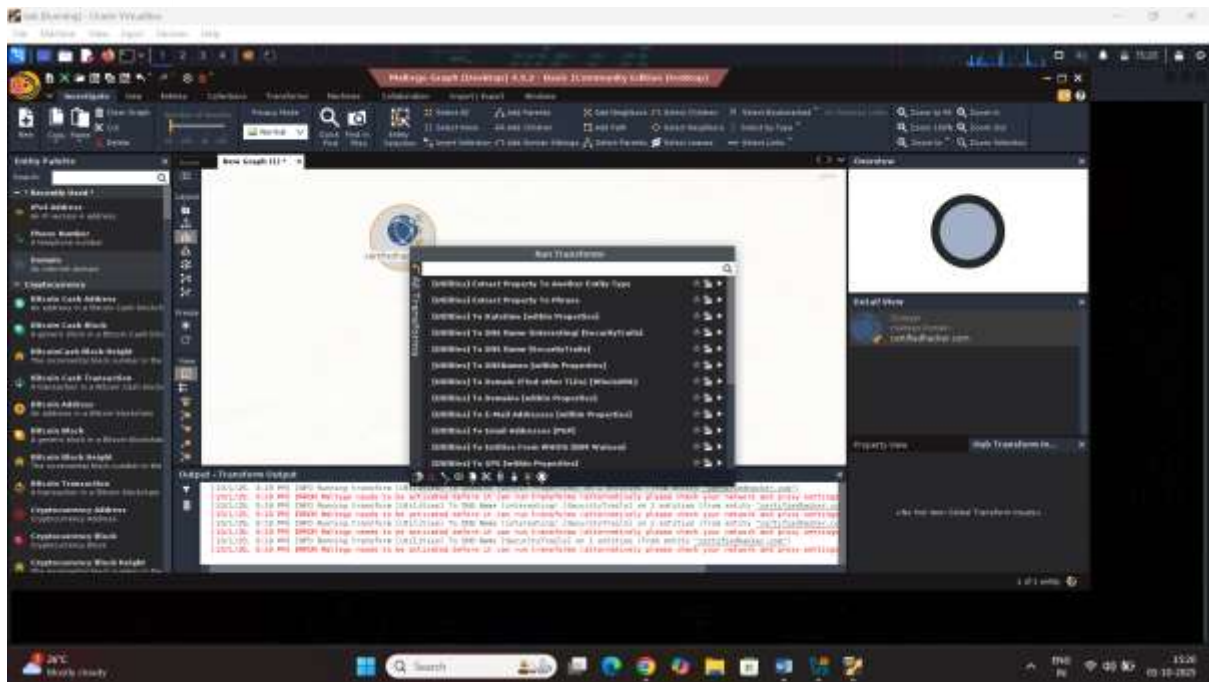
Step3 click on the new option



Step5 select the domain and drop and drag the layout



Step6 click on the wright option



Result:

