Perform open-source intelligence gathering using Net craft, Whois Lookups, DNS Reconnaissance, Harvester and Maltego

Aim:

To perform open-source intelligence gathering using Net craft, Whois Lookups, DNS Reconnaissance, Harvester and Maltego.

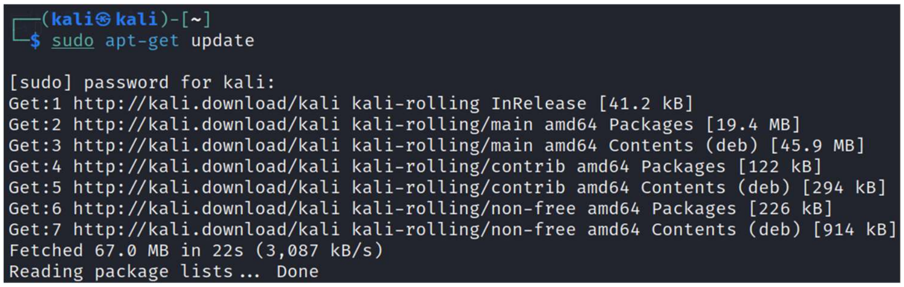
Procedure:

A. Update and Upgrade Kali Linux

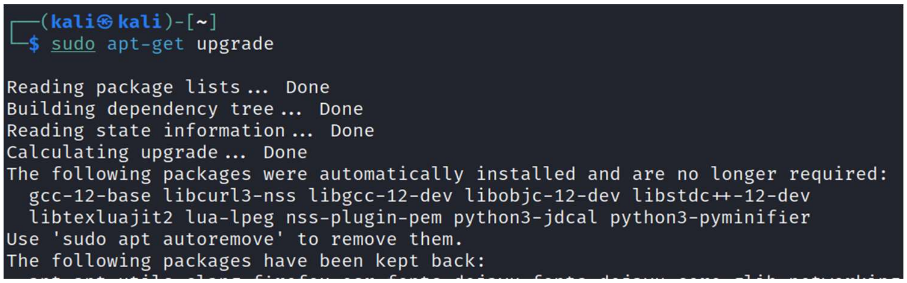
Open a terminal in Kali Linux and run the following commands to update the package lists and upgrade the system.

sudo apt-get update: Updates the package lists for upgrades and new package installations.

sudo apt-get upgrade: Upgrades the installed packages to the latest versions.



```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get update

[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.2 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.4 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [45.9 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [122 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [294 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [226 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [914 kB]
Fetched 67.0 MB in 22s (3,087 kB/s)
Reading package lists ... Done
```

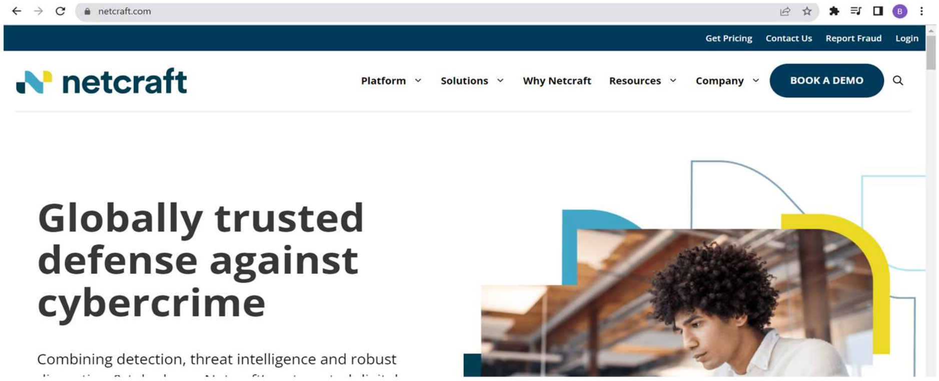


```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get upgrade

Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Calculating upgrade ... Done
The following packages were automatically installed and are no longer required:
  gcc-12-base libcurl3-nss libgcc-12-dev libobjc-12-dev libstdc++-12-dev
  libtexluajit2 lua-lpeg nss-plugin-pem python3-jdcal python3-pyminifier
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  apt apt-utils clang firefox-esr fonts-dejavu fonts-dejavu-core glib-networking
```

B. Netcraft

Netcraft, a leading internet services company, specializes in technical analyses crucial for understanding and securing the internet landscape. Through monthly Web Server Surveys, Netcraft provides comprehensive data on web server market share, aiding businesses and IT professionals in strategic decision-making. Their Anti-Phishing Services include real-time monitoring and a browser extension to combat phishing threats effectively. Additionally, Netcraft offers Site Reports, SSL/TLS Surveys, and DDoS Protection Testing, providing in-depth insights into websites' security postures.

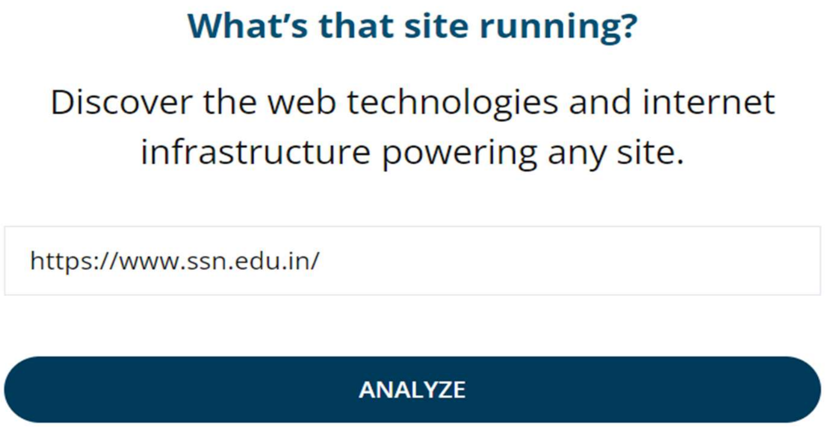
1. Visit the official website of Netcraft by https://www.netcraft.com/



Globally trusted defense against cybercrime

Combining detection, threat intelligence and robust

2. Scroll down the website. Enter the website to find the details of web technologies and internet infrastructure used. Click Analyze to display the details.

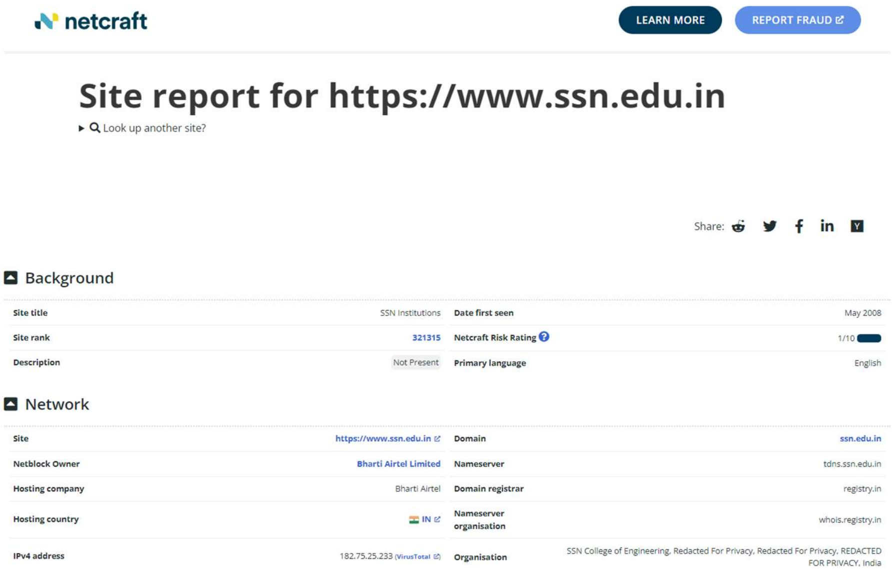


What's that site running?

Discover the web technologies and internet infrastructure powering any site.

https://www.ssn.edu.in/

3. The details are displayed as follows:



Site report for https://www.ssn.edu.in

Background

Site title	SSN Institutions	Date first seen	May 2008
Site rank	321315	Netcraft Risk Rating	1/10
Description	Not Present	Primary language	English

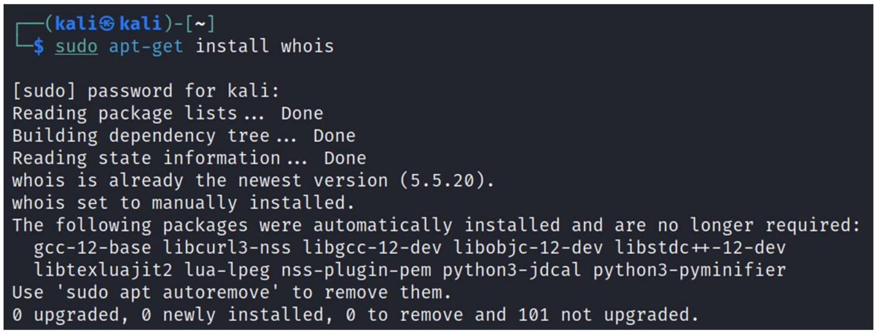
Network

Site	https://www.ssn.edu.in	Domain	ssn.edu.in
Netblock Owner	Bharti Airtel Limited	Nameserver	tdns.ssn.edu.in
Hosting company	Bharti Airtel	Domain registrar	registry.in
Hosting country	IN	Nameserver organisation	whois.registry.in
IPv4 address	182.75.25.233 (VirusTotal)	Organisation	SSN College of Engineering, Redacted For Privacy, Redacted For Privacy, REDACTED FOR PRIVACY, India

C. Whois Lookups

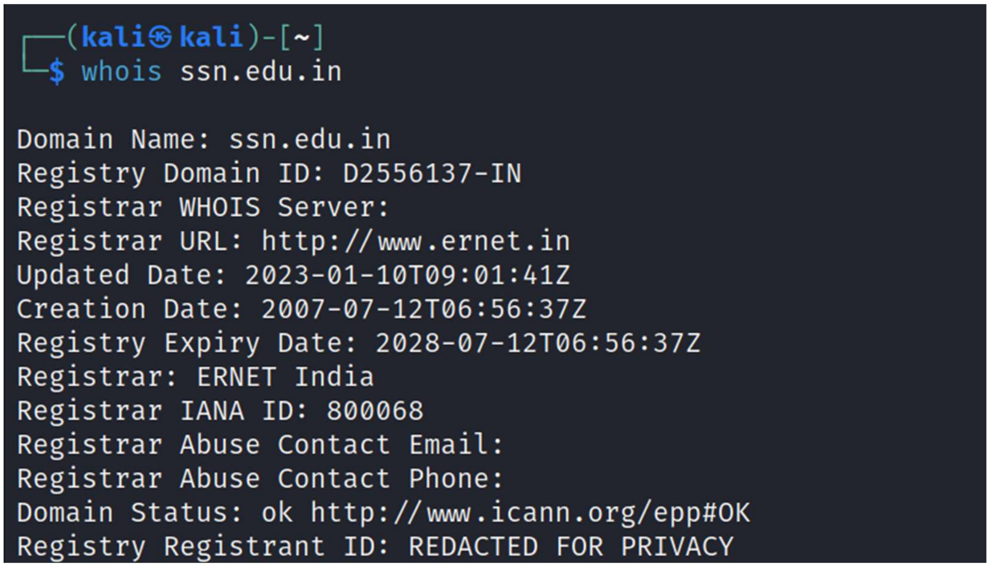
WHOIS lookup is a straightforward yet powerful tool for gathering information about a target. It provides details such as IP addresses or host names of a company's DNS servers, offering insights into its IT infrastructure. The service also furnishes contact information, including addresses and phone numbers, facilitating legitimate inquiries or addressing technical concerns. While privacy protection services may obscure actual contact details, WHOIS remains a valuable resource for cybersecurity, network management, and due diligence.

1. Open the Kali Linux Terminal. Install the Whois by the command ‘sudo apt-get install whois’



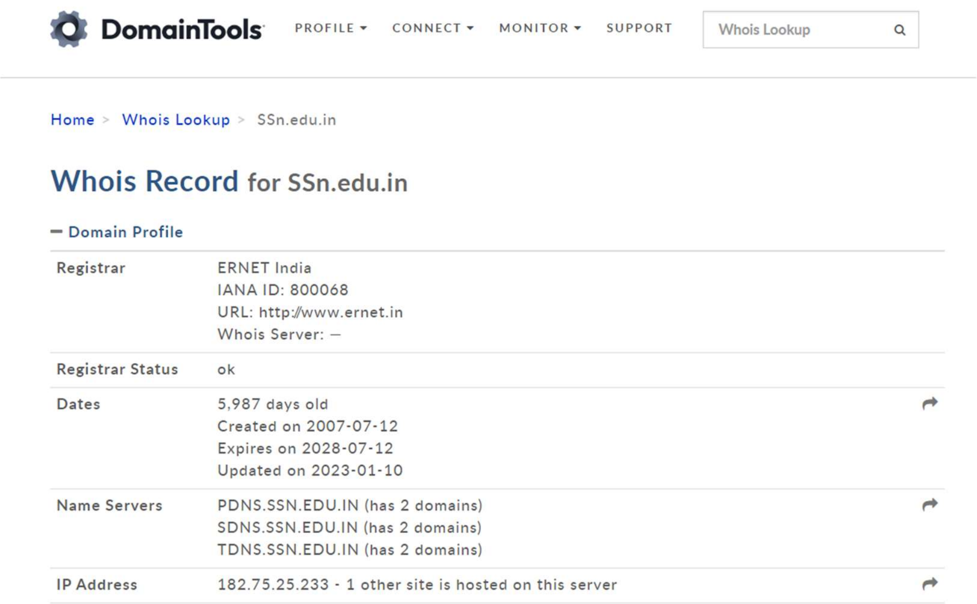
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install whois

[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
whois is already the newest version (5.5.20).
whois set to manually installed.
The following packages were automatically installed and are no longer required:
  gcc-12-base libcurl3-nss libgcc-12-dev libobjc-12-dev libstdc++-12-dev
  libtexluajit2 lua-lpeg nss-plugin-pem python3-jdcal python3-pyminifier
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 101 not upgraded.
```

2. The command ‘whois ssn.edu.in’ retrieves registration details for the domain "ssn.edu.in," including information about the registrar, registration date, and contact details of the domain owner.



```
┌──(kali㉿kali)-[~]
└─$ whois ssn.edu.in

Domain Name: ssn.edu.in
Registry Domain ID: D2556137-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2023-01-10T09:01:41Z
Creation Date: 2007-07-12T06:56:37Z
Registry Expiry Date: 2028-07-12T06:56:37Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
```

3. An alternative method to retrieve WHOIS information for the domain "ssn.edu.in" is to use the website: https://whois.domaintools.com/. Enter the Domain name in the search box field and search it.



Home > Whois Lookup > SSn.edu.in

Whois Record for SSn.edu.in

— Domain Profile

Registrar	ERNET India IANA ID: 800068 URL: http://www.ernet.in Whois Server: –
Registrar Status	ok
Dates	5,987 days old Created on 2007-07-12 Expires on 2028-07-12 Updated on 2023-01-10
Name Servers	PDNS.SSN.EDU.IN (has 2 domains) SDNS.SSN.EDU.IN (has 2 domains) TDNS.SSN.EDU.IN (has 2 domains)
IP Address	182.75.25.233 - 1 other site is hosted on this server

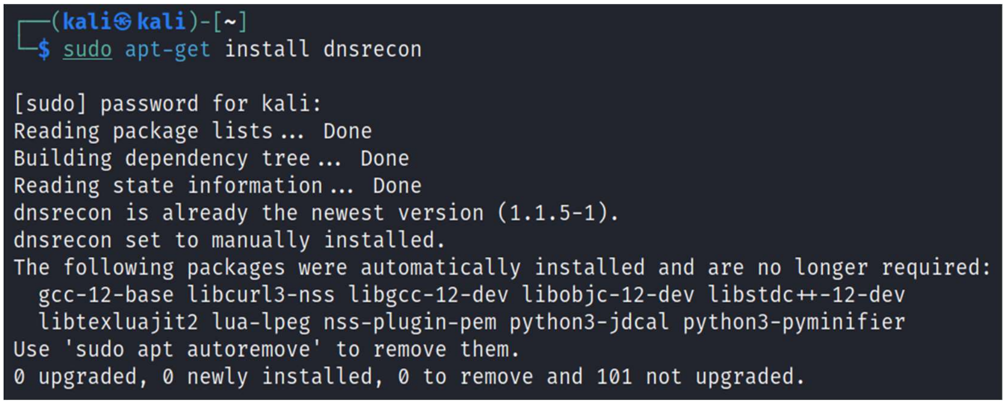
D. DNS Reconnaissance

DNS Reconnaissance involves the systematic exploration of a target's Domain Name System (DNS) to gather crucial information about its network infrastructure. This process includes identifying subdomains, attempting zone transfers, analyzing mail exchange records, and examining text and service records.

DNS reconnaissance helps reveal the target's DNS architecture, services, and potential vulnerabilities. Specialized tools like `dnsrecon` are employed for tasks such as subdomain enumeration and zone transfer attempts. The insights gained from DNS reconnaissance contribute to a better understanding of the target's attack surface, aiding security professionals in fortifying their DNS infrastructure.

1. Open a terminal and run the following command to install DNS Reconnaissance.

sudo apt-get install dnsrecon: Installs the DNS Reconnaissance tool for gathering information about DNS records.

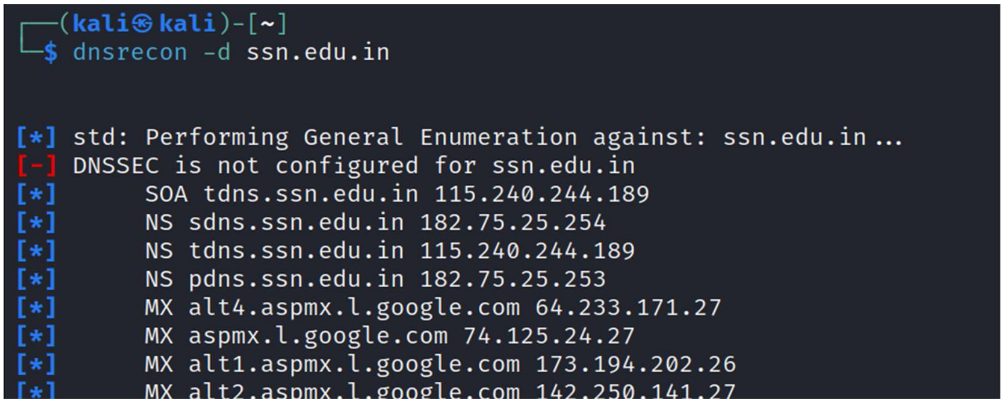


```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install dnsrecon

[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
dnsrecon is already the newest version (1.1.5-1).
dnsrecon set to manually installed.
The following packages were automatically installed and are no longer required:
  gcc-12-base libcurl3-nss libgcc-12-dev libobjc-12-dev libstdc++-12-dev
  libtexluajit2 lua-lpeg nss-plugin-pem python3-jdcal python3-pyminifier
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 101 not upgraded.
```

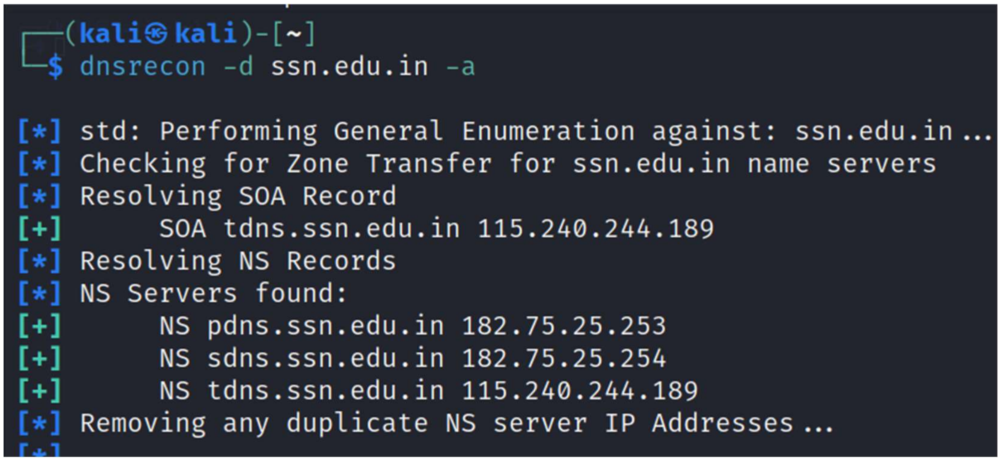
2. Run the following commands to perform DNS Reconnaissance on a specific domain.

dnsrecon -d ssn.edu.in: Performs a standard DNS reconnaissance on the specified domain ssn.edu.in.

dnsrecon -d ssn.edu.in -a: Performs a more aggressive DNS enumeration for the domain ssn.edu.in.



```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -d ssn.edu.in


[*] std: Performing General Enumeration against: ssn.edu.in ...
[-] DNSSEC is not configured for ssn.edu.in
[*]      SOA tdns.ssn.edu.in 115.240.244.189
[*]      NS sdns.ssn.edu.in 182.75.25.254
[*]      NS tdns.ssn.edu.in 115.240.244.189
[*]      NS pdns.ssn.edu.in 182.75.25.253
[*]      MX alt4.aspmx.l.google.com 64.233.171.27
[*]      MX aspmx.l.google.com 74.125.24.27
[*]      MX alt1.aspmx.l.google.com 173.194.202.26
[*]      MX alt2.aspmx.l.google.com 142.250.141.27
```



```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -d ssn.edu.in -a

[*] std: Performing General Enumeration against: ssn.edu.in ...
[*] Checking for Zone Transfer for ssn.edu.in name servers
[*] Resolving SOA Record
[+]      SOA tdns.ssn.edu.in 115.240.244.189
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS pdns.ssn.edu.in 182.75.25.253
[+]      NS sdns.ssn.edu.in 182.75.25.254
[+]      NS tdns.ssn.edu.in 115.240.244.189
[*] Removing any duplicate NS server IP Addresses ...
```

E. Harvester

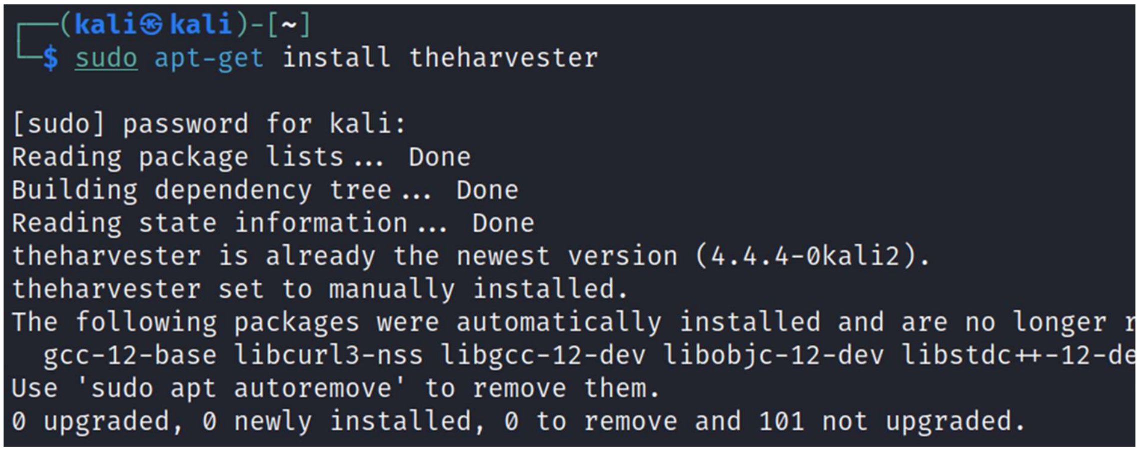
An excellent tool to use in reconnaissance is the Harvester. The Harvester is a powerful Open-Source Intelligence (OSINT) tool designed for reconnaissance and information gathering. It facilitates the extraction of valuable data such as email addresses, subdomains, hostnames, employee names, and more from various public sources.

The Harvester can be used to search Google, Bing, and PGP servers for emails, hosts, and subdomains.

- “-d” is used to specify the target domain.
- “-l” is used to limit the number of results returned to us.
- “-b” is used to specify the public repository.

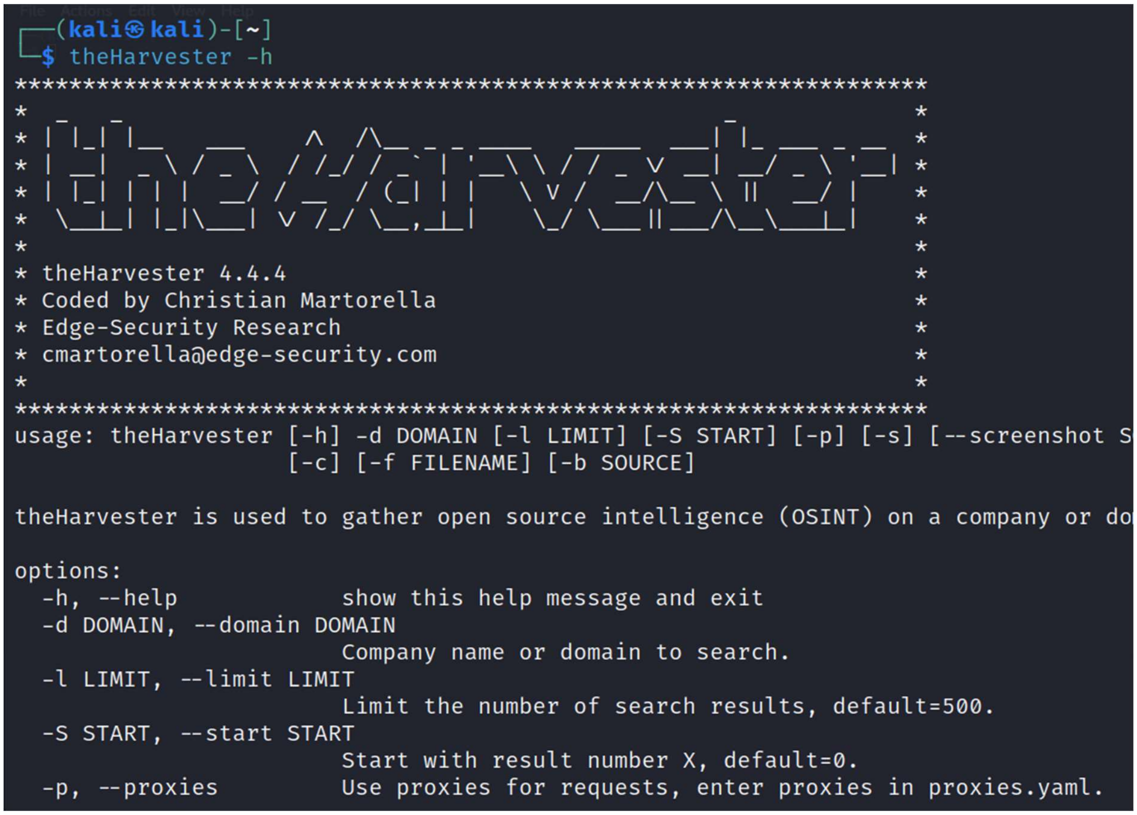
Open a terminal and run the following commands to install and use Harvester:

sudo apt-get install theharvester: Installs the Harvester tool on a Debian-based system.



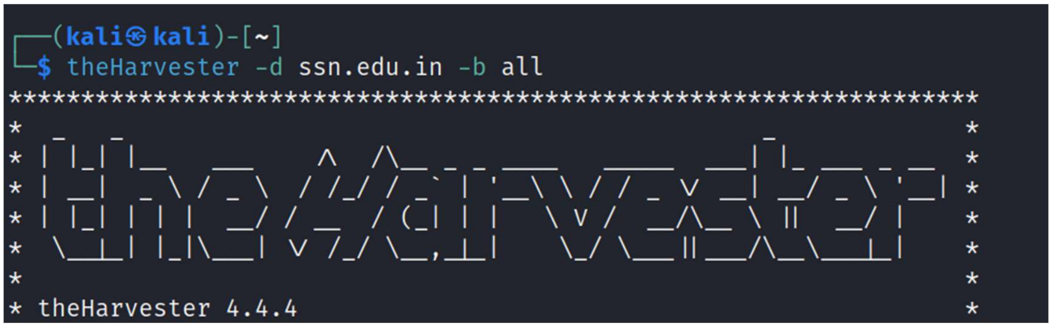
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install theharvester

[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
theharvester is already the newest version (4.4.4-0kali2).
theharvester set to manually installed.
The following packages were automatically installed and are no longer r
  gcc-12-base libcurl3-nss libgcc-12-dev libobjc-12-dev libstdc++-12-de
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 101 not upgraded.
```

theHarvester -h: Displays the tool's help menu, providing details on available commands and options.



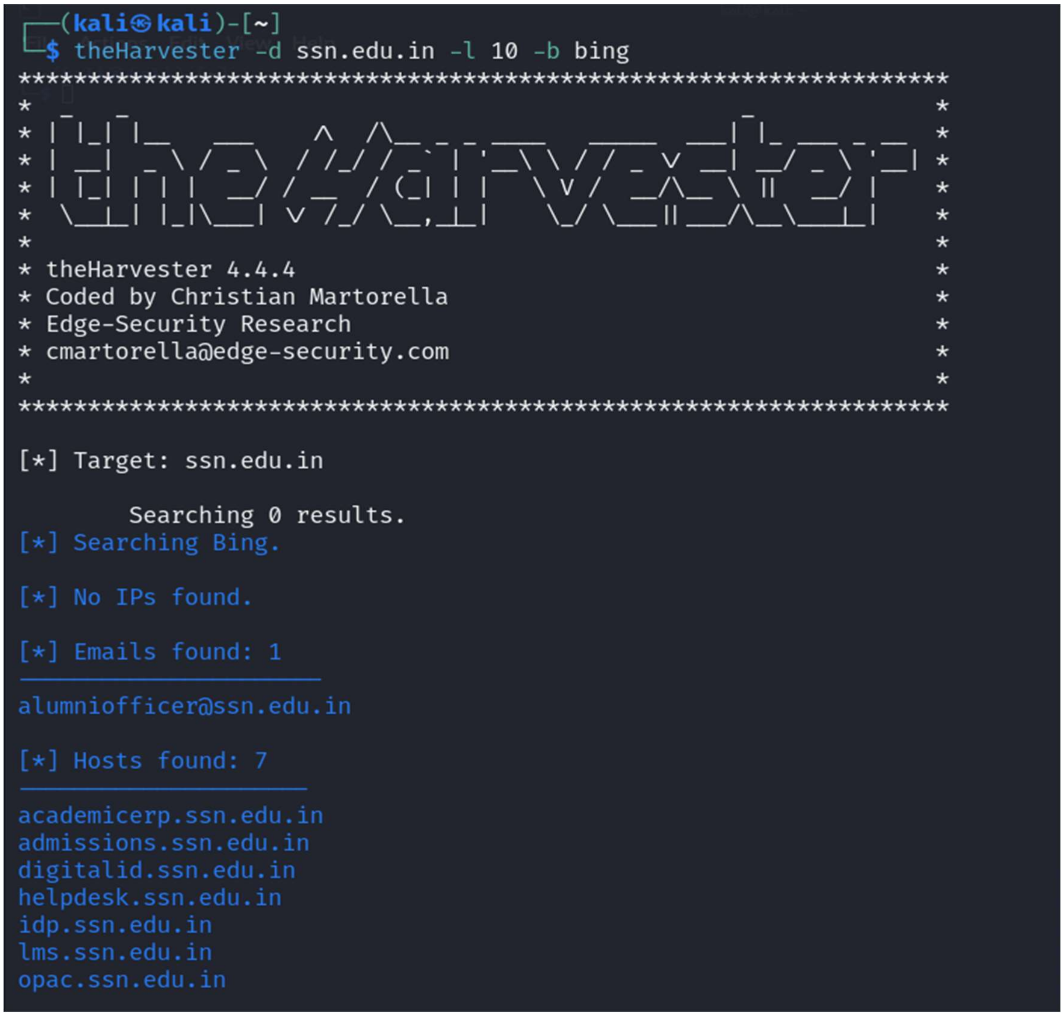
```
┌──(kali㉿kali)-[~]
└─$ theHarvester -h
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.4.4                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************
usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-p] [-s] [--screenshot S
                    [-c] [-f FILENAME] [-b SOURCE]

theHarvester is used to gather open source intelligence (OSINT) on a company or do

options:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Company name or domain to search.
  -l LIMIT, --limit LIMIT
                        Limit the number of search results, default=500.
  -S START, --start START
                        Start with result number X, default=0.
  -p, --proxies         Use proxies for requests, enter proxies in proxies.yaml.
```

theHarvester -d ssn.edu.in -b all: Gathers information on the domain ssn.edu.in using all available sources, providing a comprehensive OSINT report.



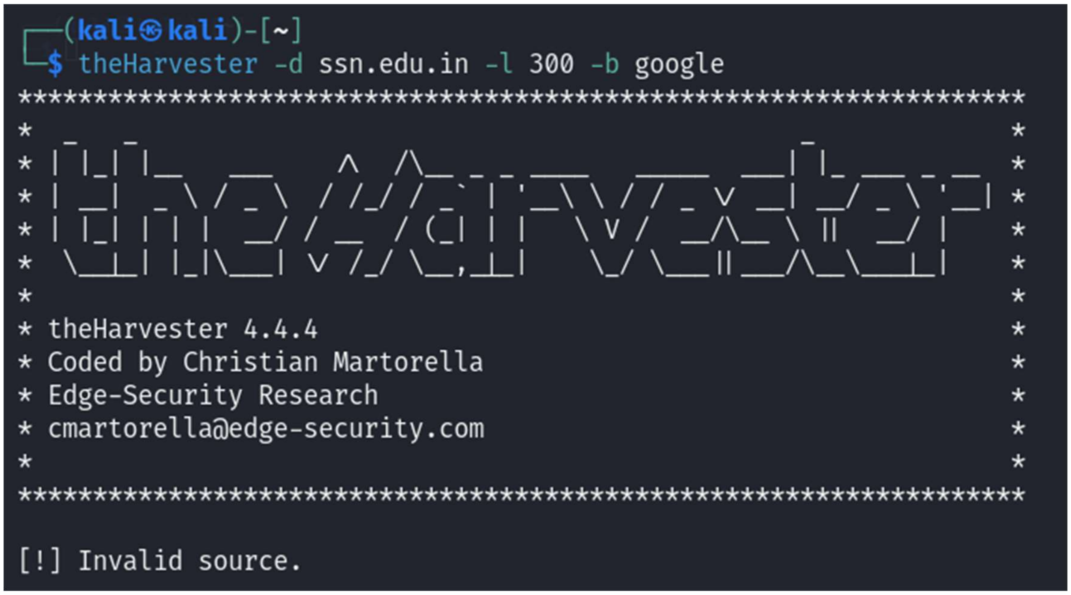
```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d ssn.edu.in -b all
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.4.4                                              *
```

theHarvester -d ssn.edu.in -l 10 -b bing: Limits the search to 10 results and specifically uses Bing as the source for OSINT data on the domain.



```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d ssn.edu.in -l 10 -b bing
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.4.4                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: ssn.edu.in

        Searching 0 results.
[*] Searching Bing.

[*] No IPs found.

[*] Emails found: 1
----------------------
alumniofficer@ssn.edu.in

[*] Hosts found: 7
---------------------
academicerp.ssn.edu.in
admissions.ssn.edu.in
digitalid.ssn.edu.in
helpdesk.ssn.edu.in
idp.ssn.edu.in
lms.ssn.edu.in
opac.ssn.edu.in
```

theHarvester -d ssn.edu.in -l 300 -b google: Limits the search to 300 results and specifically uses Google as the source for OSINT data on the domain.



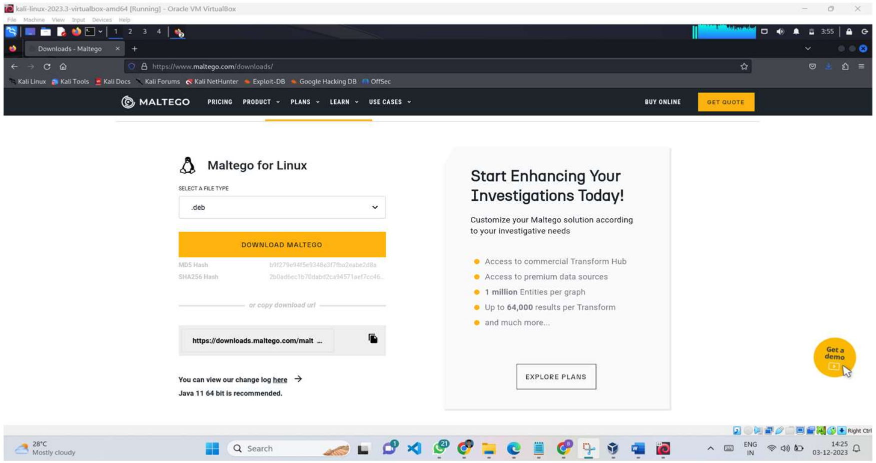
```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d ssn.edu.in -l 300 -b google
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.4.4                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[!] Invalid source.
```

F. Maltego

Maltego, developed by Paterva, is an Open-Source Intelligence (OSINT) powerhouse, transforming information gathering into a visual experience. With a graph-based approach, it unveils complex relationships between data points, integrating seamlessly with diverse sources.

Key features include customizable transforms, link analysis, and collaborative capabilities. Maltego finds applications in footprinting, threat intelligence, and social engineering defense, making it a go-to tool for cybersecurity professionals. Users navigate ethical use and continuous learning to harness its full potential in revealing hidden connections and insights.

1. Download Maltego from the official website https://www.maltego.com/downloads/



Maltego for Linux

SELECT A FILE TYPE

.deb

DOWNLOAD MALTEGO

MD5 Hash b9f279e94f5e9348e3f7fba2eabe2d8a

SHA256 Hash 2b0ad6ec1b70dabd2ca94571aef7cc46...

or copy download url

https://downloads.maltego.com/malt ...

You can view our change log here →

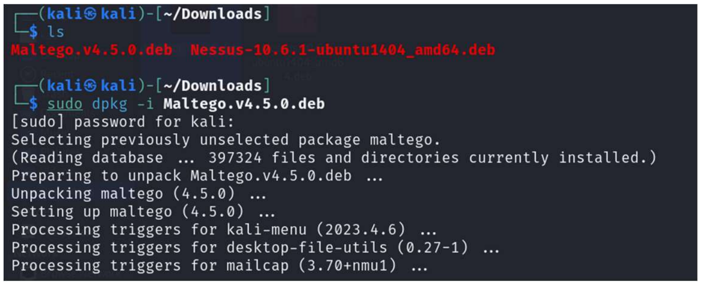
Java 11 64 bit is recommended.

Start Enhancing Your Investigations Today!

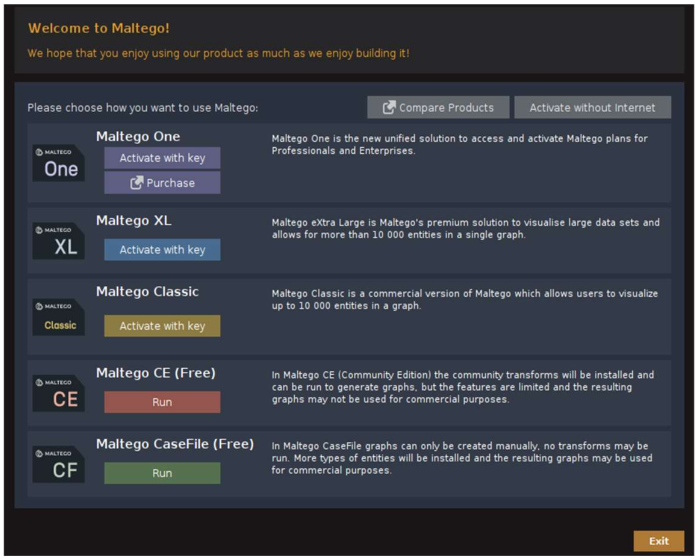
Customize your Maltego solution according to your investigative needs

- Access to commercial Transform Hub
- Access to premium data sources
- **1 million** Entities per graph
- Up to **64,000** results per Transform
- and much more...

2. Install Maltego for Linux. Choose the Maltego CE (Free) and create your account and login the account.



```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
Maltego.v4.5.0.deb  Nessus-10.6.1-ubuntu1404_amd64.deb

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i Maltego.v4.5.0.deb
[sudo] password for kali:
Selecting previously unselected package maltego.
(Reading database ... 397324 files and directories currently installed.)
Preparing to unpack Maltego.v4.5.0.deb ...
Unpacking maltego (4.5.0) ...
Setting up maltego (4.5.0) ...
Processing triggers for kali-menu (2023.4.6) ...
Processing triggers for desktop-file-utils (0.27-1) ...
Processing triggers for mailcap (3.70+nmu1) ...
```



Welcome to Maltego!

We hope that you enjoy using our product as much as we enjoy building it!

Please choose how you want to use Maltego:

Maltego One

Maltego One is the new unified solution to access and activate Maltego plans for Professionals and Enterprises.

Maltego XL

Maltego eXtra Large is Maltego's premium solution to visualise large data sets and allows for more than 10 000 entities in a single graph.

Maltego Classic

Maltego Classic is a commercial version of Maltego which allows users to visualize up to 10 000 entities in a graph.

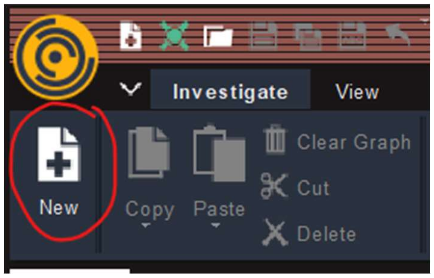
Maltego CE (Free)

In Maltego CE (Community Edition) the community transforms will be installed and can be run to generate graphs, but the features are limited and the resulting graphs may not be used for commercial purposes.

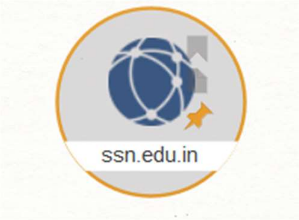
Maltego CaseFile (Free)

In Maltego CaseFile graphs can only be created manually, no transforms may be run. More types of entities will be installed and the resulting graphs may be used for commercial purposes.

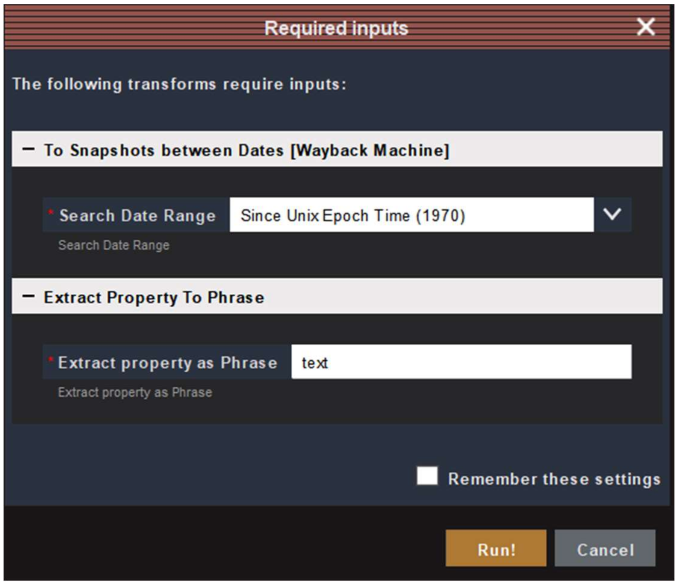
3. Click New to create a new graph.



4. In the left Entity Palette search for ‘Domain’ and then drag and drop on the graph and rename to ‘ssn.edu.in’.



5. Right click and select the run icon in ‘All Transforms’. Click Run in the below popup.


Required inputs

The following transforms require inputs:

− To Snapshots between Dates [Wayback Machine]

* Search Date Range: Since Unix Epoch Time (1970)

Search Date Range

− Extract Property To Phrase

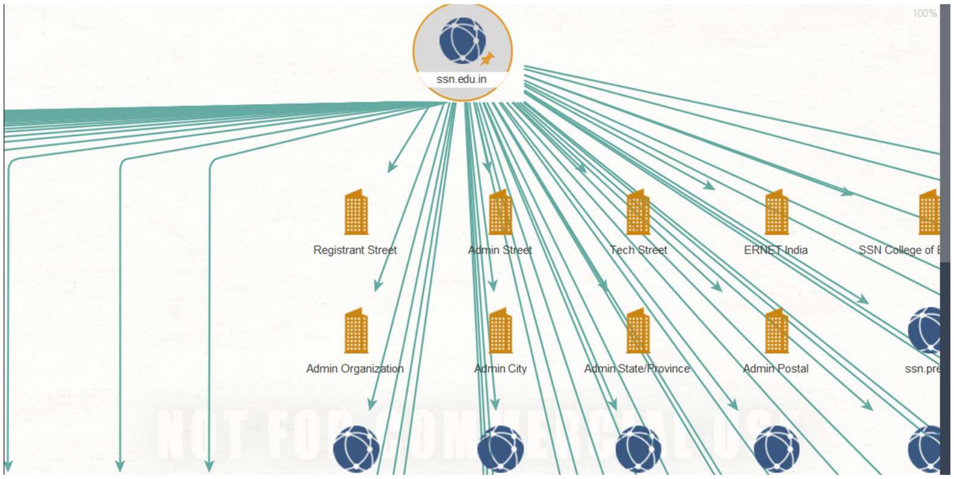
* Extract property as Phrase: text

Extract property as Phrase

□ Remember these settings

Run! Cancel

6. Now a detailed graph will be displayed as follows.



Result

In this exercise, we've learned to conduct effective open-source intelligence (OSINT) gathering using tools like Netcraft, WHOIS lookups, DNS reconnaissance, the Harvester, and Maltego. This includes analyzing web technologies, retrieving domain registration details, exploring network infrastructure, extracting valuable data from public sources, and visualizing complex relationships between data points. These skills are essential for cybersecurity professionals to assess and enhance the security of online entities.