

# Hacking Articles

Raj Chandel's Blog

[Author](#)[Web Penetration Testing](#)[Penetration Testing](#)[Courses We Offer](#)[My Books](#)[Donate us](#)

**POST CATEGORY :** Footprinting

Search

## Beginner Guide to Website Footprinting

posted in [FOOTPRINTING](#) on [JULY 23, 2017](#) by [RAJ CHANDEL](#) with [0 COMMENT](#)

In our [previous](#) article we have discussed a brief introduction of footprinting for gathering information related to the specific person. As we had discussed that there are so many type of footprinting and today we are going to talk about DNS footprinting, website footprinting and whois footprinting.

**Browsing the target Website may Providing**

Whos is Details

Subscribe to Blog via Email

**SUBSCRIBE**

Software used and version

OS Details

Sub Domains

File Name and File Path

Scripting Platform & CMS Details

Contact Details

**Let's start!!**

**From Wikipedia**

**Whois footprinting**

WHOIS (pronounced as the phrase who is) is a query and response protocol and whois footprinting is a method for glance information about ownership of a domain name as following:

- Domain name details
- Contact details contain phone no. and email address of owner
- Registration date for domain name
- Expire date for domain name
- Domain name servers

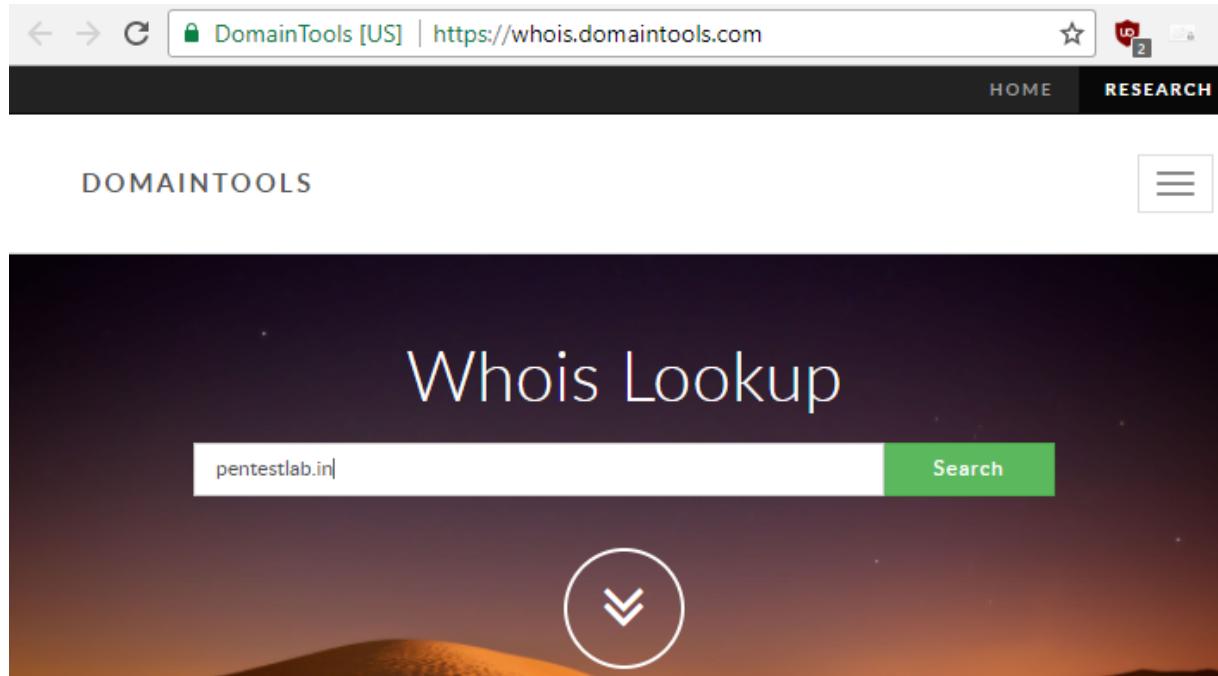
## **Whois Lookup**

It is broadly used in support of querying databases that store the registered users or assignees of an Internet resource, such as a **domain name**, an **IP address block**, or an **autonomous system**, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format.



Browse given URL <http://whois.domaintools.com> in browser and type any domain name.

For example: let's search **pentestlab.in**



Now you can see it has created a whois record for **pentestlab.in** where it contains details like: **email address, IP, registrant Org**. From given record anyone can guess that this domain have some connection to raj chandel. Then attacker needs to perform footprinting on raj chandel taking help from previous article.

There is so many other tools use for whois footprinting for example:

- **Caller IP**
- **Whois Analyzer pro**
- **Whois lookup multiple address**

## Categories

- ❑ [BackTrack 5 Tutorials](#)
- ❑ [Best of Hacking](#)
- ❑ [Browser Hacking](#)
- ❑ [Cryptography & Stegnography](#)
- ❑ [CTF Challenges](#)
- ❑ [Cyber Forensics](#)
- ❑ [Database Hacking](#)
- ❑ [Domain Hacking](#)
- ❑ [Email Hacking](#)
- ❑ [Footprinting](#)
- ❑ [Hacking Tools](#)
- ❑ [Kali Linux](#)
- ❑ [Nmap](#)
- ❑ [Others](#)
- ❑ [Penetration Testing](#)
- ❑ [Social Engineering Toolkit](#)
- ❑ [Trojans & Backdoors](#)
- ❑ [Website Hacking](#)
- ❑ [Window Password Hacking](#)
- ❑ [Windows Hacking Tricks](#)
- ❑ [Wireless Hacking](#)
- ❑ [Youtube Hacking](#)

## Whois Record for PentesLab.in

### - Whois & Quick Stats

Email	rrajchandel@gmail.com is associated with ~8 domains	↗
Registrant Org	RAJ Chandel is associated with ~2 other domains	↗
Dates	Created on 2017-07-11 - Expires on 2018-07-11 - Updated on 2017-07-11	↗
IP Address	72.52.229.111 - 120 other sites hosted on this server	↗
IP Location	🇺🇸 - Michigan - Lansing - Liquid Web L.L.C	↗
ASN	AS32244 LIQUID-WEB-INC - Liquid Web, L.L.C, US (registered Mar 26, 2004)	↗
Whois History	3 records have been archived since 2017-07-11	↗
Whois Server	whois.inregistry.net	↗

### - Website

Website Title	Ignite lab	↗
---------------	------------	---

## DNS Footprinting

Attacker performs DNS footprinting in order to enumerate DNS record details and type of servers. There are 10 type of DNS record which provide important information related to target location.

1. A/AAAA
2. SVR
3. NS
4. TXT
5. MX
6. CNAME
7. SOA
8. RP
9. PTR

## Articles

Select Month

## Facebook Page



Be the first of your friends to like this

## 10. HINFO

**Domain Dossier:** it is an online tool use for complete DNS footprinting as well as whois footprinting.

There are so many online tool use for DNS footprinting , using domain dossier we will check for DNS records of penetstlab.in, select the check box for **DNS records** and **traceroute** and then click on **go**.

The screenshot shows a web browser window with the URL <https://centralops.net/co/domaindossier.aspx>. The page title is "Domain Dossier" with the subtitle "Investigate domains and IP addresses". A search bar contains the domain "pentestlab.in". Below the search bar are several checkboxes: "domain whois record" (unchecked), "DNS records" (checked), "traceroute" (checked), "network whois record" (unchecked), and "service scan" (unchecked). A "go" button is located next to the service scan checkbox. At the bottom left, there is user information: "user: anonymous [122.180.189.187]" and "balance: 50 units", along with links for "log in" and "account info". The Central Ops .net logo is at the bottom right.

You can observe that, the data which we received from whois lookup and from domain dossier is same in some extent. It has given same email ID as above i.e.

[rrajchandel@gmail.com](mailto:rrajchandel@gmail.com)and moreover details of DNS records TXT, SOA, NS, MX, A and PTR.

## DNS records

name	class	type	data	time to live
pentestlab.in	IN	TXT	v=spf1 +a +mx +ip4:72.52.218.232 ~all	14400s (04:00:00)
pentestlab.in	IN	SOA	server: dns1.rightdns.com email: rrajchandel@gmail.com serial: 2017071105 refresh: 3600 retry: 7200 expire: 1209600 minimum ttl: 86400	86400s (1.00:00:00)
pentestlab.in	IN	NS	dns2.rightdns.com	86400s (1.00:00:00)
pentestlab.in	IN	NS	dns11.rightdns.com	86400s (1.00:00:00)
pentestlab.in	IN	NS	dns1.rightdns.com	86400s (1.00:00:00)
pentestlab.in	IN	NS	dns12.rightdns.com	86400s (1.00:00:00)
pentestlab.in	IN	A	72.52.229.111	14400s (04:00:00)
pentestlab.in	IN	MX	preference: 0 exchange: pentestlab.in	14400s (04:00:00)
111.229.52.72.in-addr.arpa	IN	PTR	sun.rightdns.com	3600s (01:00:00)
229.52.72.in-addr.arpa	IN	NS	ns1.sourcedns.com	300s (00:05:00)

**DNS Dumpster:** it is also an online use for DNS footprinting.

**DNSdumpster.com** is a FREE domain research tool that can discover hosts related to a domain. Enumerate a domain and pull back up to 40K subdomains, results are available in a XLS for easy reference.

Repeating same process for **pentestlab.in**, it will search for its DNS record. From given screenshot you can observe we have received same details as above. More it will create a copy as output file in from XLS.

The screenshot shows a web browser displaying the results of a DNS dump for the domain `pentestlab.in`. The results are categorized into several sections:

- DNS Servers:** Lists four entries, all pointing to the IP `72.52.205.50` and the domain `sun.rightdns.com`, which is associated with AS32244 Liquid Web, L.L.C. in the United States. Each entry includes a small icon with a red exclamation mark.
- MX Records:** Shows one entry for the domain `pentestlab.in` with the priority `0`, pointing to the IP `72.52.229.111` and the domain `sun.rightdns.com`, also associated with AS32244 Liquid Web, L.L.C. in the United States.
- TXT Records:** Contains the command `"v=spf1 +a +mx +ip4:72.52.218.232 ~all"`.
- Host Records (A):** Lists one entry for the domain `pentestlab.in`, which points to the IP `72.52.229.111` and the domain `sun.rightdns.com`, both associated with AS32244 Liquid Web, L.L.C. in the United States.

**You get signal:** it is also an online tool use for DNS footprinting as well as for Network footprinting

A **reverse IP domain check** takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on that same web server. Data is gathered from search engine results, which are not guaranteed to be complete

Hence we get the **IP 72.52.229.111** for **pentestlab.in** moreover it dumped the name of **14** other domain which are hosted on same web server.

# you get signal

## Reverse IP Domain Check



Remote Address

Found 14 domains hosted on the same web server as [pentestlab.in](#) (72.52.229.111).

[ganeshdiagnostic.org](#)  
[kobraindia.com](#)  
[neelgirimachinery.com](#)  
[sseengg.com](#)  
[www.blackinkanimation.com](#)  
[www.sarswatimachinetools.com](#)  
[www.vkhomedecor.com](#)

[ignitetechnologies.in](#)  
[kobramumbai.com](#)  
[pentestlab.in](#)  
[tptl.in](#)  
[www.ignitetechnologies.in](#)  
[www.steemo.com](#)  
[yestradingco.com](#)

## Website Footprinting

It is technique use for extracting the details related to website as following

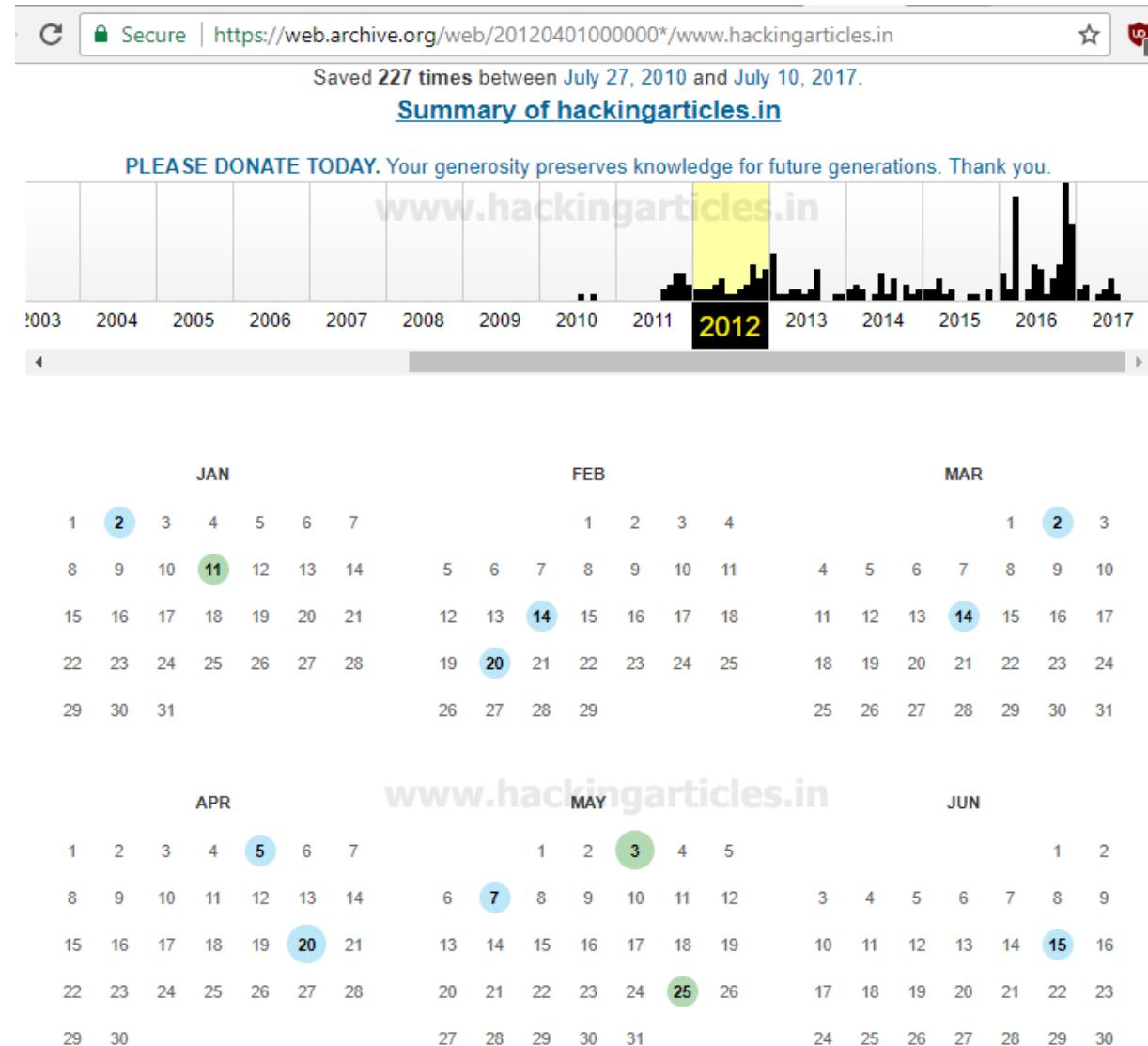
1. Archived description of website
2. Content management system and framework
3. Script and platform of the website and webserver
4. Web crawling
5. Extract meta data and contact details from website
6. Website and web page monitoring and analyzer

**Archive.org:** It is an online tool use for visiting **archived version** of any website.

Archive.org has search option as **wayback machine** which is like a time machine for any website. It contains entire information from past till present scenario of any website either

their layout or content everything related to website is present inside. In simple words it contains history of any website.

For example I had search for [hackingarticles.in](https://web.archive.org/web/20120401000000*/www.hackingarticles.in) archived record of 2012.



**Built With:** It is an online tool used for detecting techniques and framework involved inside running website.

[BuiltWith.com](#) technology tracking includes widgets, analytics, frameworks, content management systems, advertisers, content delivery networks, web standards and web servers to name some of the technology categories.

Taking example of [hackingarticles.in](#) again we found following things:

- Content Management system: **WordPress**
- Framework: **PHP**

[Log In](#) · [Sign Up for Free](#)



Tools ▾

Features ▾

Plans & Pricing

Customers

Resources ▾

## Content Management Systems

[View Global Trends](#)

### WordPress

[WordPress Usage Statistics - Download list of all WordPress websites ⓘ](#)

WordPress is a state-of-the-art semantic personal publishing platform with a focus on aesthetics, web standards, and usability.

### WordPress Weekly Activity

[WordPress Weekly Activity Usage Statistics - Download list of all WordPress Weekly Activity websites ⓘ](#)

### Wordpress 4.7

[Wordpress 4.7 Usage Statistics - Download list of all Wordpress 4.7 websites ⓘ](#)

### Wordpress 4.8

[Wordpress 4.8 Usage Statistics - Download list of all Wordpress 4.8 websites ⓘ](#)

## Frameworks

[View Global Trends](#)

### PHP

[PHP Usage Statistics - Download list of all PHP websites ⓘ](#)

PHP is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.

## Advertising

[View Global Trends](#)

### eXelate

## Whatweb

Whatweb can identify all sorts of information about a live website, like: Platform, CMS platform, Type of Script, Google Analytics, Webserver Platform, and IP address Country. A

pentester can use this tool as both a recon tool & vulnerability scanner.

Open the terminal in kali Linux and type following command

**Whatweb** [www.pentestlab.in](http://www.pentestlab.in)

As result we receive same information as above

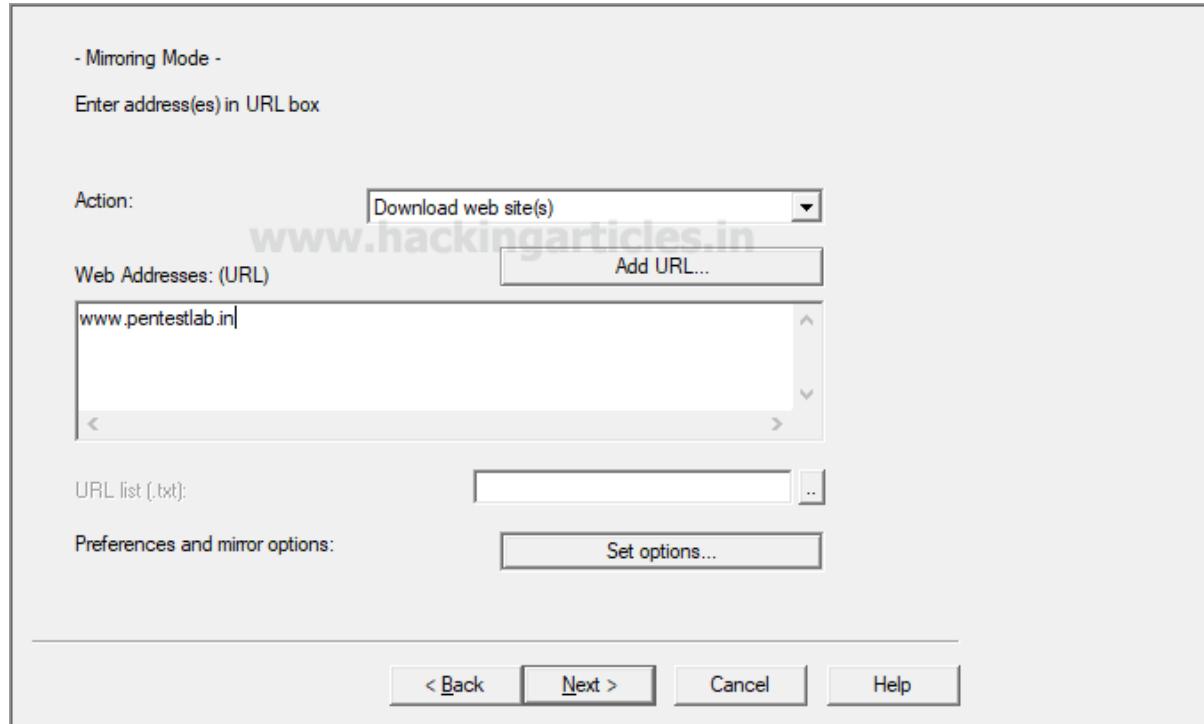
```
root@kali:~# whatweb www.pentestlab.in
http://www.pentestlab.in [200 OK] Apache, Country[UNITED STATES][US], HTML5, HTT
PServer[Apache], IP[72.52.229.111], JQuery, Script, Title[Ignite lab]
```

## Web crawling

**HTTrack** is a free and open source Web crawler and offline browser, developed by Xavier Roche

It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer. HTTrack arranges the original site's relative link-structure.

Give target URL for copy the web site as [www.pentestlab.in](http://www.pentestlab.in) which starts downloading the website.

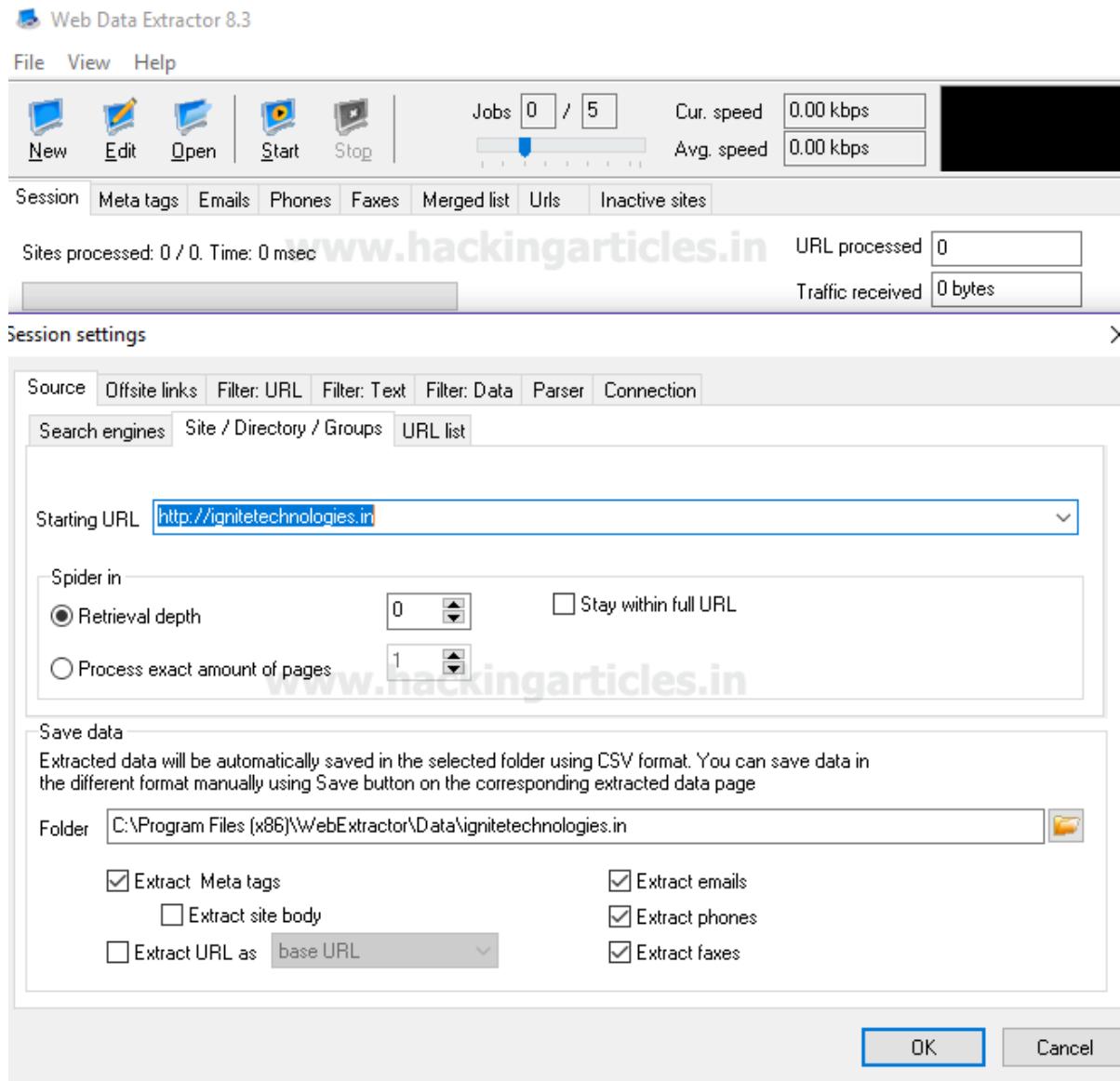


<http://www.hackingarticles.in/5-ways-crawl-website/>

## Web Data Extractor

**Web Data Extractor Pro** is a web scraping tool specifically designed for mass-gathering of various data types. It can **harvest URLs, phone and fax numbers, email addresses**, as well as meta tag information and body text. Special feature of WDE Pro is custom extraction of structured data.

Start new project Type target URL as ignitetechologies.in and select folder to save the output and click on **ok**.

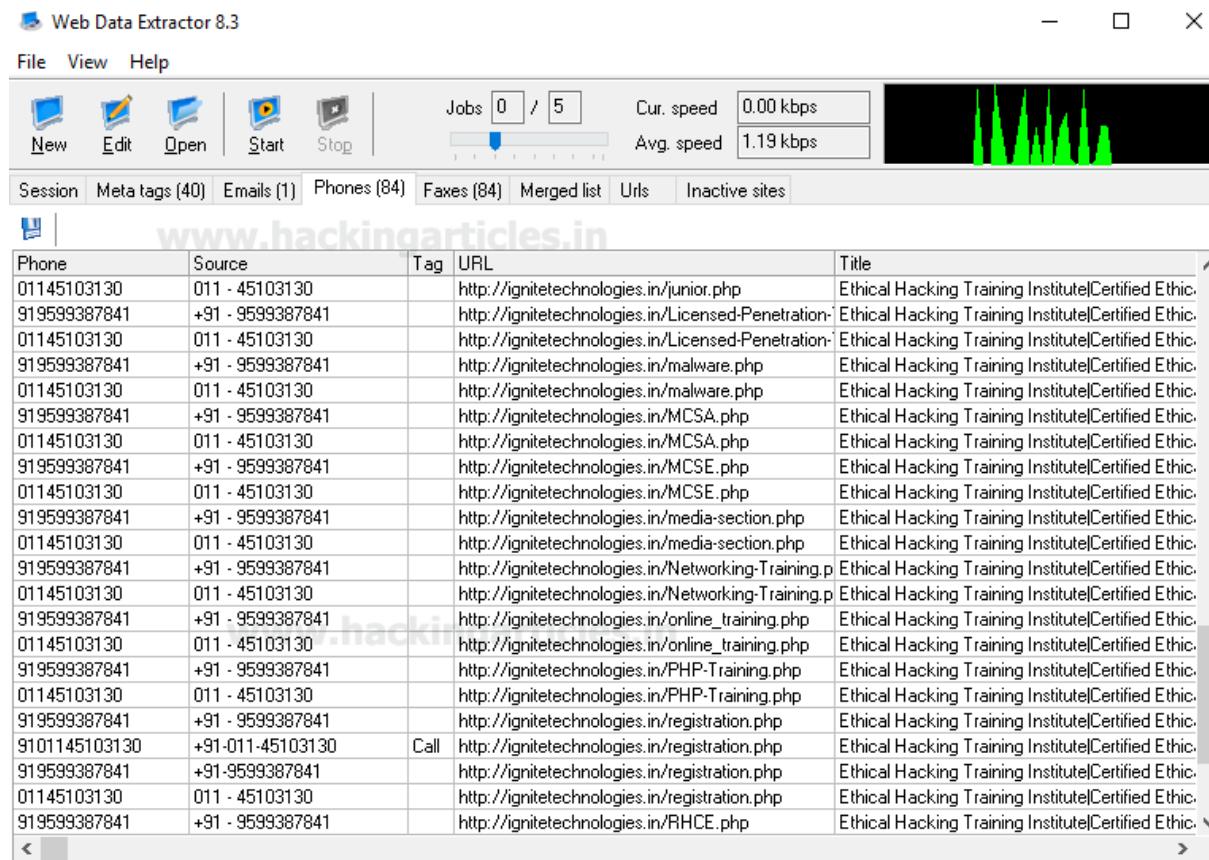


Now this tool will extract meta data, email contact no. and etc from inside the target URL.

From given screenshot you can see it found **40 meta tags** **1 email** **84-phone number** from ignitetechologies.in website.

Similarly there other tool use as web data extractor:

## Web spider



The screenshot shows the Web Data Extractor 8.3 application window. At the top, there's a menu bar with File, View, and Help, and a toolbar with New, Edit, Open, Start, and Stop buttons. Below the toolbar, a status bar displays 'Jobs 0 / 5', 'Cur. speed 0.00 kbps', and 'Avg. speed 1.19 kbps'. A progress bar with green peaks is shown. The main area has tabs for Session, Meta tags (40), Emails (1), Phones (84), Faxes (84), Merged list, URLs, and Inactive sites. The Phones tab is selected, displaying a table with columns: Phone, Source, Tag, URL, and Title. The table lists numerous entries from 'www.hackingarticles.in' related to ethical hacking training and certifications.

Phone	Source	Tag	URL	Title
01145103130	011 - 45103130		http://ignitechnologies.in/junior.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitechnologies.in/Licensed-Penetration-	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitechnologies.in/Licensed-Penetration-	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitechnologies.in/malware.php	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitechnologies.in/malware.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitechnologies.in/MCSA.php	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitechnologies.in/MCSA.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitechnologies.in/MCSE.php	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitechnologies.in/MCSE.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitechnologies.in/media-section.php	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitechnologies.in/media-section.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitechnologies.in/Networking-Training.p	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitechnologies.in/Networking-Training.p	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitechnologies.in/online_training.php	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitechnologies.in/online_training.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitechnologies.in/PHP-Training.php	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitechnologies.in/PHP-Training.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitechnologies.in/registration.php	Ethical Hacking Training Institute Certified Ethic.
9101145103130	+91-011-45103130	Call	http://ignitechnologies.in/registration.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91-9599387841		http://ignitechnologies.in/registration.php	Ethical Hacking Training Institute Certified Ethic.
01145103130	011 - 45103130		http://ignitechnologies.in/registration.php	Ethical Hacking Training Institute Certified Ethic.
919599387841	+91 - 9599387841		http://ignitechnologies.in/RHCE.php	Ethical Hacking Training Institute Certified Ethic.

## Competitive Intelligence

Website-Watcher is a **powerful yet simple website-monitoring tool**, perfectly suited to the beginner and advanced user alike. You can download it from [here](#).

Using **new** tab and enter target URL which start monitoring the target website.

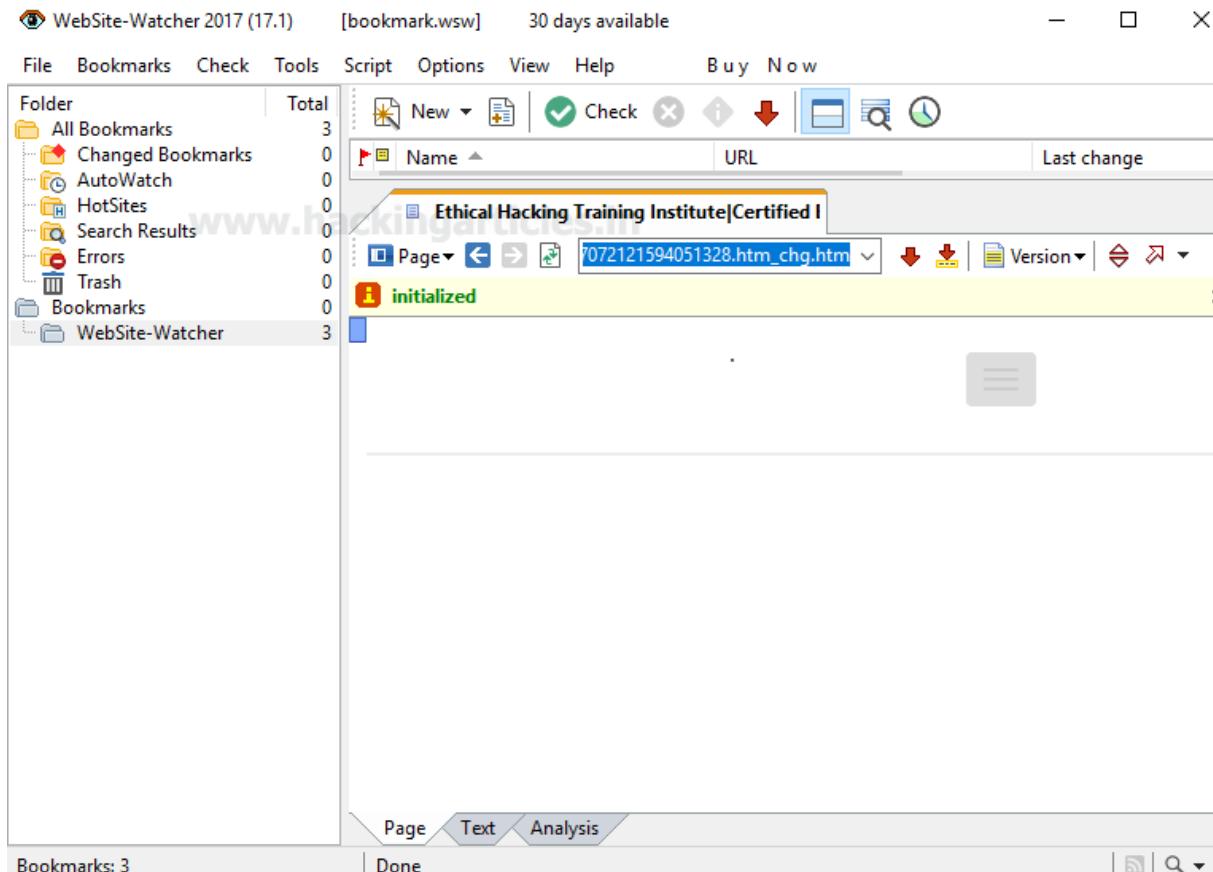
For example I enter URL `hackingarticles.in` for monitoring this website.

Similarly there are some other tool uses for monitoring:

**On web change**

**Follow that page**

**Informinder**



**Author:** AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)

# 5 ways to Banner Grabbing

posted in **FOOTPRINTING** , **PENETRATION TESTING** on **JULY 12, 2017** by **RAJ CHANDEL**  
with **0 COMMENT**

**Banner** are refers as text message that received from host. Banners usually contain information about a service, such as the version number.

From Wikipedia

**Banner grabbing** is a process to collect details regarding any remote PC on a network and the services running on its open ports. An attacker can make use of banner grabbing in order to discover network hosts and running services with their versions on their open ports and more over operating systems so that he can exploits it.

## Nmap

A simple banner grabber which connects to an open TCP port and prints out anything sent by the listening service within five seconds.

The banner will be shortened to fit into a single line, but an extra line may be printed for every increase in the level of verbosity requested on the command line.

Type following command which will fetch banner for every open port in remote PC.

```
1 | nmap -sV --script=banner 192.168.1.106
```

From screenshot you can read the services and their version for open ports fetched by NMAP Script to grab banner for the target 192.168.1.106

```
root@kali:~# nmap -sV --script=banner 192.168.1.106
Starting Nmap 7.50 ( https://nmap.org ) at 2017-07-12 10:09 EDT
Nmap scan report for 192.168.1.106
Host is up (0.0043s latency)
```

```
host is up (0.0043s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ banner: 220 (vsFTPD 2.3.4)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
23/tcp    open  telnet       Linux telnetd
|_ banner: \xFF\xFD\x18\xFF\xFD \xFF\xFD#\xFF\xFD'
25/tcp    open  smtp         Postfix smtpd
|_ banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     2 (RPC #100000)
|_ rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp    rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp   nfs
|   100005  1,2,3     55010/udp  mountd
|   100005  1,2,3     56414/tcp  mountd
|   100021  1,3,4     37454/udp  nlockmgr
|   100021  1,3,4     41196/tcp  nlockmgr
|   100024  1          36246/udp  status
|   100024  1          37643/tcp  status
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
|_ banner: \x01Where are you?
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  shell       Metasploitable root shell
|_ banner: root@metasploitable:#
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
|_ banner: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.106]
```

Following command will grab the banner for selected port i.e. **80** for http service and version.

```
1 | nmap -Pn -p 80 -sV --script=banner 192.168.1.106
```

As result it will dumb “http-server-header: Apache/2.2.8 (Ubuntu) DAV/2”

```
root@kali:~# nmap -Pn -p 80 -sV --script=banner 192.168.1.106
Starting Nmap 7.50 ( https://nmap.org ) at 2017-07-12 10:16 EDT
Nmap scan report for 192.168.1.106
Host is up (0.0066s latency).

PORT      STATE SERVICE VERSION
80/tcp      open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
MAC Address: 38:B1:DB:B3:BC:D9 (Hon Hai Precision Ind.)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.41 seconds
```

## CURL

Curl -I is use for head in order to shown document information only; type following command to grab **HTTP banner** of remote PC.

```
1 | curl -s -I 192.168.1.106 | grep -e "Server: "
```

As result it will dumb “http-server-header: Apache/2.2.8 (Ubuntu) DAV/2”

```
root@kali:~# curl -s -I 192.168.1.106 | grep -e "Server: "
Server: Apache/2.2.8 (Ubuntu) DAV/2
root@kali:~#
```

## Telnet

Type following command to grab **SSH banner** of remote PC.

```
1 | telnet 192.168.1.106 22
```

As result it will dumb “SSH-2.0-OpenSSH\_4.7p1 Debian-8ubuntu1”

```
oot@kali:~# telnet 192.168.1.106 22
Trying 192.168.1.106...
Connected to 192.168.1.106.
Escape character is '^]'.
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

## Netcat

Type following command to grab **SSH banner** of remote PC.

```
1 | nc -v 192.168.1.106 22
```

As result it will dumb “SSH-2.0-OpenSSH\_4.7p1 Debian-8ubuntu1”

```
root@kali:~# nc -v 192.168.1.106 22
192.168.1.106: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.1.106] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

## Dmitry

DMitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU)Linux Command Line Application coded in C. DMitry has the ability to gather as much information as possible about a host. Base functionality is able to gather possible subdomains, email addresses, uptime information, tcp port scan, whois lookups, and more.

Dmitry **-b** is use for banner grabbing for all open ports; Type following command to grab **SSH banner** of remote PC.

```
1 | dmitry -b 192.168.1.106
```

From screenshot you can see it has shown banner for open port **21, 22, 23** and **25**.

In this way Attacker can grab the services and their version for open ports on remote PC

```
root@kali:~# dmitry -b 192.168.1.106
Deepmagic Information Gathering Tool
"There be some deep magic going on"
Error: No '-p' flag passed with TTL, assuming -p
ERROR: Unable to locate Host Name for 192.168.1.106
Continuing with limited modules
HostIP:192.168.1.106
HostName:

Gathered TCP Port information for 192.168.1.106
-----
Port          State
21/tcp        open
>> 220 (vsFTPD 2.3.4)
22/tcp        open
>> SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

23/tcp        open
>> 00:00:00#00'
25/tcp        open
>> 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

**Author:** AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)

## Beginner Guide to Footprinting

posted in **FOOTPRINTING** on **JUNE 20, 2017** by **RAJ CHANDEL** with **0 COMMENT**

There are many saying about know your enemy, time and time again these saying have proved to be true. Today we hear all around the work of hackers and many-a-times we fail to protect ourselves. This happens because we are not familiar of their working process. Therefore, in this article we are here to make to accustomed to the first step of the process i.e. Footprinting.

In the world of Cyber Security, Footprinting is the first step which lets penetration testers gather information about hardware or network. It is basically an exploration process which helps us to know our enemy. In order to complete penetration process, one ought to gather as much information as possible. Footprinting can be done either actively or passively. Assessing a company's website with their permission is an illustration of passive footprinting and trying to access sensitive information through social engineering is an illustration of active information gathering.

#### **Types of Footprinting:**

- Footprinting through Search Engine
- Footprinting through social engineering
- Footprinting through Social Networking sites
- Website Footprinting
- Competitive Intelligence
- WHOIS Footprinting
- Footprinting using advanced Google hacking techniques
- Email Footprinting
- DNS Footprinting
- Network Footprinting

As this is the first part of our footprinting series, we will discuss first three types of footprinting.

## Footprinting through Search Engine

Footprinting through search engine is unambiguous in itself. People often wonder what one can find through search engine as the common concept of search engine is basic exploring. But results given by search engine can be used to hacker's advantage as they are vast in nature.

Attackers use search to gather information about their target such as technology platforms, employee details, log in pages, intranet portals, etc. which helps in performing social engineering and/or other types of advanced system attacks.

Even search engine cache and internet archives may provide sensitive information that has been removed from World Wide Web (WWW).

There are many search engines where you can find anything that desire from finding a meaning of the word to finding a person. Such search engines are:

[www.google.com](http://www.google.com)

[www.bing.com](http://www.bing.com)

[www.shodan.io](http://www.shodan.io)

[www.duckduckgo.com](http://www.duckduckgo.com)

Now let's take example of [google.com](http://www.google.com). If I search "Raj Chandel" in Google, then it will give me every possible result associated with the said person.

The screenshot shows a Google search results page for the query "Raj Chandel". The search bar at the top contains "Raj Chandel". Below the search bar, there are tabs for All, News, Videos, Images, Maps, More, and Settings. The "All" tab is selected. The search results section starts with a message: "About 3,61,000 results (0.64 seconds)". The first result is a link to "Raj Chandel | Professional Profile - LinkedIn" with the URL <https://in.linkedin.com/in/raj-chandel-a8178717>. The snippet below the link reads: "New Delhi Area, India - Founder & CTO Hacking Articles - IGNITE TECHNOLOGIES View Raj Chandel's professional profile on LinkedIn. LinkedIn is the world's largest business network helping professionals like Raj Chandel discover inside ...". The second result is a link to "Hacking Articles,Ethical Hacking Training in Delhi,Metasploit Training" with the URL [www.hackingarticles.in/](http://www.hackingarticles.in/). The snippet below the link reads: "Hacking Articles is a very interesting blog about information security, penetration testing and vulnerability assessment managed by Raj Chandel. In this blog it's ... Penetration Testing · Facebook Hacking · Table of Contents · Kali Linux".

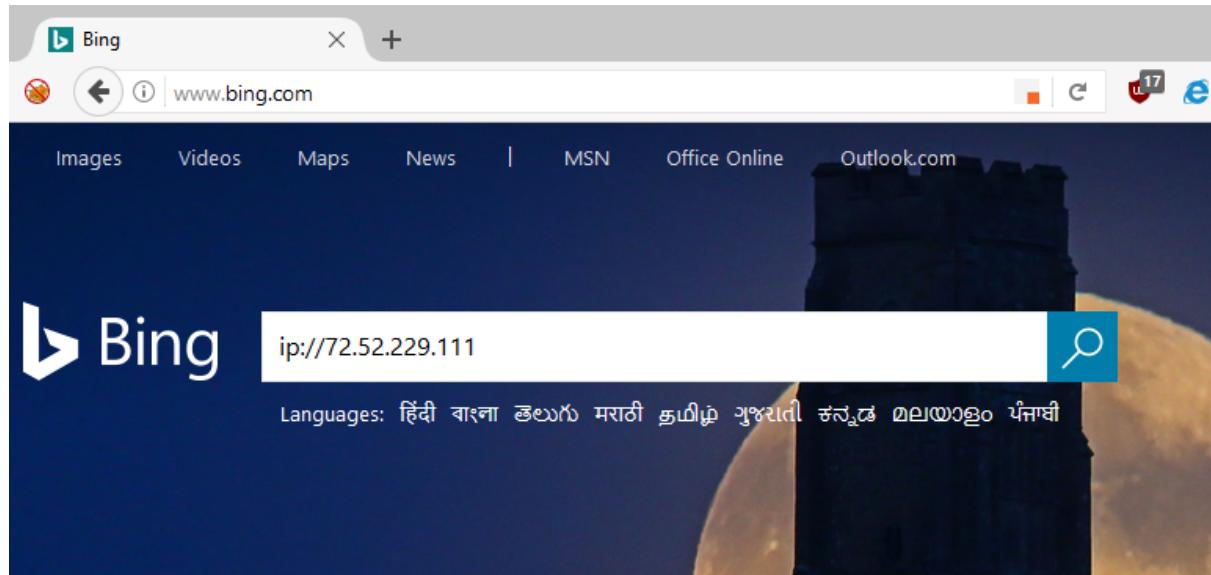
Same will be the result from other search engines. But different search engines are often used for particular searches. As shown above Google is good for general information. If you want to know that which websites are hosted on a particular server then you can use Bing search engine. To know an IP address of any website just ping the website as shown below :

```
C:\Users\RAJ>ping ignitetechologies.in

Pinging ignitetechologies.in [72.52.229.111] with 32 bytes of data:
Reply from 72.52.229.111: bytes=32 time=302ms TTL=48
Reply from 72.52.229.111: bytes=32 time=290ms TTL=48
Reply from 72.52.229.111: bytes=32 time=302ms TTL=48
Reply from 72.52.229.111: bytes=32 time=293ms TTL=48

Ping statistics for 72.52.229.111:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 290ms, Maximum = 302ms, Average = 296ms
```

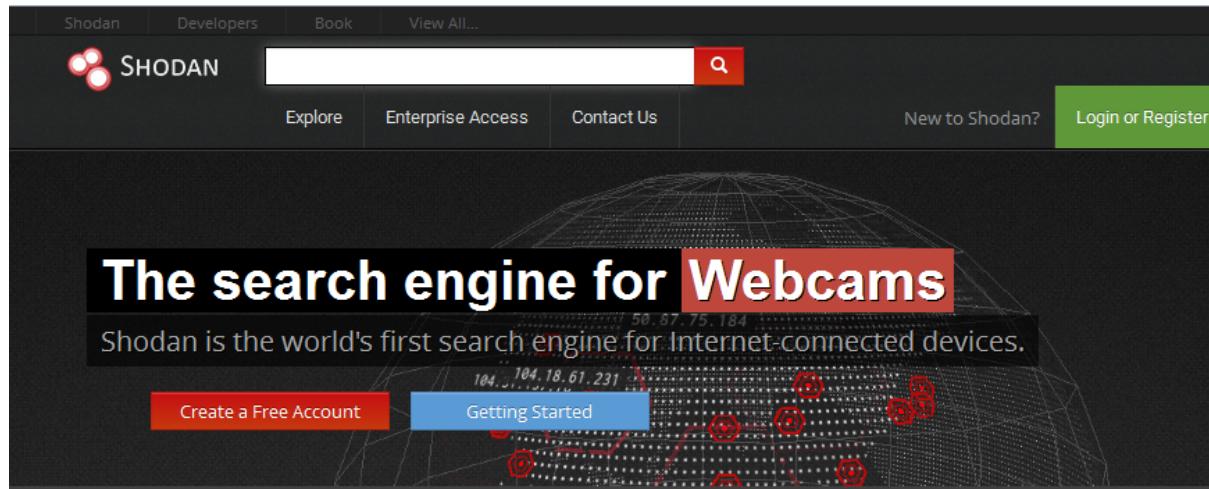
Now, open [bing.com](http://bing.com) and type the IP in the search tab and press enter.



So like this, Bing can give you details about websites which are hosted in same server

A screenshot of a web browser window showing the search results for the IP address "ip://72.52.229.111" on Bing. The search bar at the top shows the query "ip://72.52.229.111 - Bing". The results page displays 7,830 results. The first result is for "TPTL - Broadband Internet Service Provider" with a link to "www.tptl.in". The second result is for "Ganesh Diagnostic &amp; Imaging Centre Pvt. Ltd" with a link to "ganeshdiagnostic.org". Both results include a brief description and a snippet of the website's content.

Another search engine is shodan.io, it helps to locate various open ports, vulnerable IP's, and effected digital-ware all over the world. Open shodan.io in your browser and search for port or IP.



#### Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



#### See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



#### Monitor Network Security



#### Get a Competitive Advantage

For a detailed tutorial of shodan.io please follow this link:

<http://www.hackingarticles.in/shodan-search-engine-hackers-beginner-tutorial/>

#### Footprinting through jobs seeking sites

Similarly, you can collect abundance of information through job sites. You can know about company's infrastructure details, employee's profile, hardware information, software information. Some of such sites are:

[www.monster.com](http://www.monster.com)

<http://www.careerbuilder.co.in/>

[www.dice.com](http://www.dice.com)

[www.simplyhired.com](http://www.simplyhired.com)

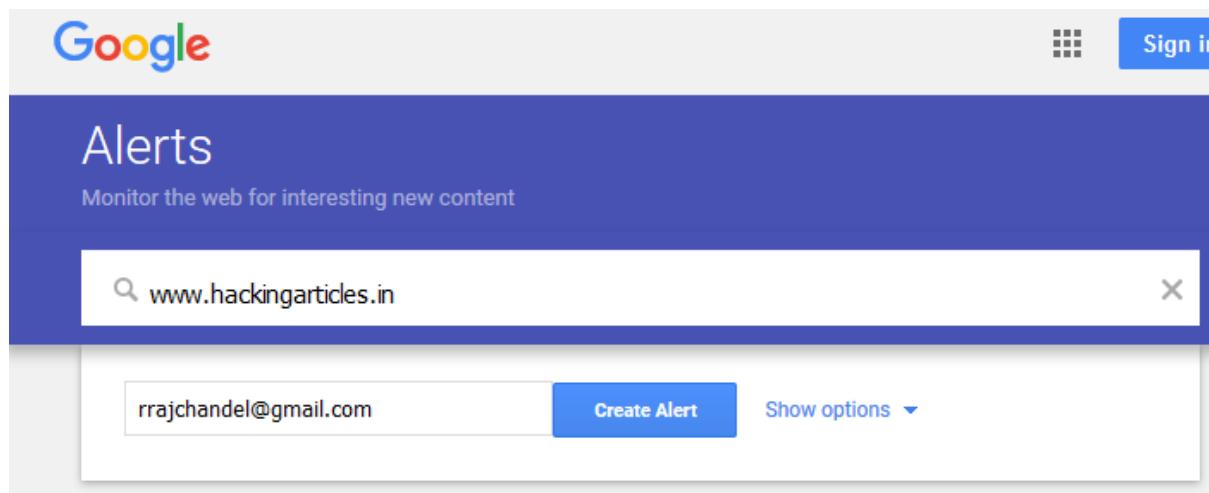
[www.indeed.com](http://www.indeed.com)

[www.usajobs.gov](http://www.usajobs.gov)

[www.naukri.com](http://www.naukri.com)

### **Footprinting through Alerts**

There is also a feature of adding alerts. This feature gives you an alert if anything is changed in particular website; given that you have added an alert to the said website. To do so, open [google.com/alerts](http://google.com/alerts) and type the name of the website that you wanted to alerted about. And then click on create alert.



And this way an alert will be created.

# Alerts

Monitor the web for interesting new content

 Create an alert about...

## My alerts (1)

hackingarticles.in



## Footprinting through Social Networking sites

Attackers use social networking sites like Facebook, Twitter, and Pinterest etc. to gain important and sensitive data about their target. They often create fake profiles through these social media to lure their target and extract vulnerable information.

Employees may post personal information such as DOB, educational and employment background, spouse's names, etc. and information about their company such as potential clients and business partners, trade secrets of business, websites, company's upcoming news, mergers, acquisitions, etc.

Even the information about the employee's interest is tracked and then they are tricked into revealing more information.

Now if you want to search particular person using just their name or email then there are specialized websites for it like [pipl.com](https://pipl.com) and [lullar.com](https://lullar.com)

Open [pipl.com](https://pipl.com) and type the name of the person you want to search about. For instance I have searched my own name and as you can see in the image below we get positive result.

The screenshot shows a web browser window for Pipl, Inc [US] at the URL <https://pipl.com/search/?q=yashika+dhir&l=&>. The search bar contains the query "yashika dhir". Below the search bar are two dropdown menus: "Location" and "Advanced". The main content area displays search results for "Yashika Dhir". The first result is a sponsored contact for "Yashika Dhir" from Delhi, India, associated with "apeejay college" and a LinkedIn icon. The second result is for "Yashika Dhir, yashikadhir4" from pinterest.com, associated with "Virtual Pinboard - Pinterest" and a Pinterest icon.

Now open [lullar.com](https://lullar.com), here you can search for people using their email and much more. Here, I have searched through email (using my own email) and there are positive result in the image below.



Profile Search by Email (ex. name@gmail.com), First Last Name or Username

yashikadhir4@gmail.com

Lullar Com Search

[Spokeo](#)

[http://www.spokeo.com/email-search/search?  
g=email\\_pt\\_lullar\\_text\\_0131&e=yashikadhir4@gmail.com](http://www.spokeo.com/email-search/search?g=email_pt_lullar_text_0131&e=yashikadhir4@gmail.com)

[Instagram](#)

<https://instagram.com/yashikadhir4>

[Facebook](#)

<http://www.facebook.com/search/results.php?q=yashikadhir4@gmail.com>

[Twitter](#)

<http://twitter.com/#!/search/yashikadhir4@gmail.com>

[YouTube](#)

[http://www.youtube.com/results?search\\_query=yashikadhir4@gmail.com](http://www.youtube.com/results?search_query=yashikadhir4@gmail.com)

[Line Add](#)

<http://line.me/R/ti/p/~yashikadhir4>

[Line QR](#)

<http://line.me/ti/p/~yashikadhir4>

[WeChat](#)

[http://v.qq.com/search.html?ms\\_key=yashikadhir4](http://v.qq.com/search.html?ms_key=yashikadhir4)

[Google Plus](#)

<https://plus.google.com/s/yashikadhir4/people>

[LinkedIn](#)

<http://www.linkedin.com/in/yashikadhir4>

yashikadhir4@gmail.com



## Footprinting through social engineering

Social engineering is an art of manipulating human behavior to our own advantage. This proves most helpful when the need of extraction of confidential information. To do so, we have to depend on the fact that people are unaware of their valuable information and have no idea about being exploited. The most common example for this is when people call as fake credit/debit card companies and try to extract information.

### Techniques used for social engineering are:

Eavesdropping

Shoulder surfing

Dumpster diving

## Impersonation on social networking sites

This is how footprinting is done through search engines, social networking sites and social engineering. As white hat hackers we should know about it but we should also be aware try to protect ourselves from black hat hackers against footprinting.

**Author:** Yashika Dhir is a passionate Researcher and Technical Writer at Hacking Articles. She is a hacking enthusiast. contact [here](#)

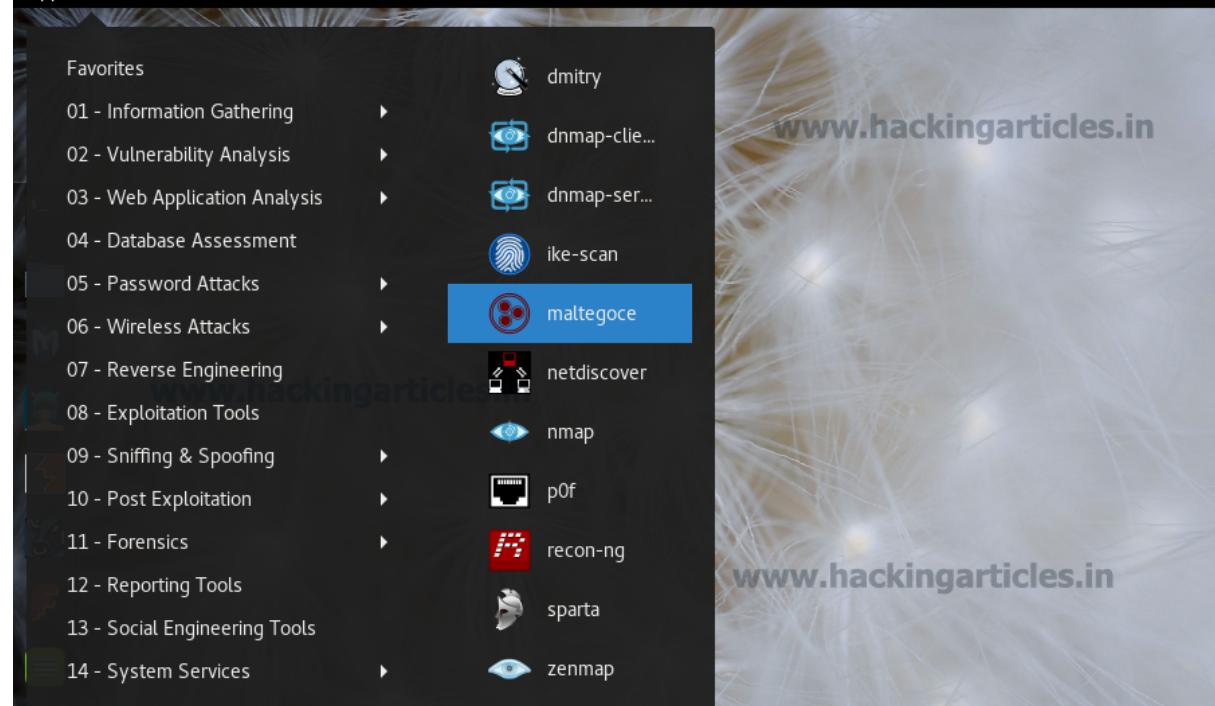
## Information Gathering using Maltego (Beginner Guide)

posted in **FOOTPRINTING** , **HACKING TOOLS** , **PENETRATION TESTING** on **MAY 8, 2016**  
by **RAJ CHANDEL** with **0 COMMENT**

Maltego is a great tool for penetration testers and forensic investigator's which is used for open-source intelligence gathering and forensics. Maltego is totally different and powerful from other intelligence gathering tool because it discovers and collects data about the target and visualizes that collected data in a wonderful graph format for analysis.

So, let's see how to use it for intelligence gathering.

Here I'm using Maltego in kali Linux. Go to **application-Information Gathering - maltegoce**

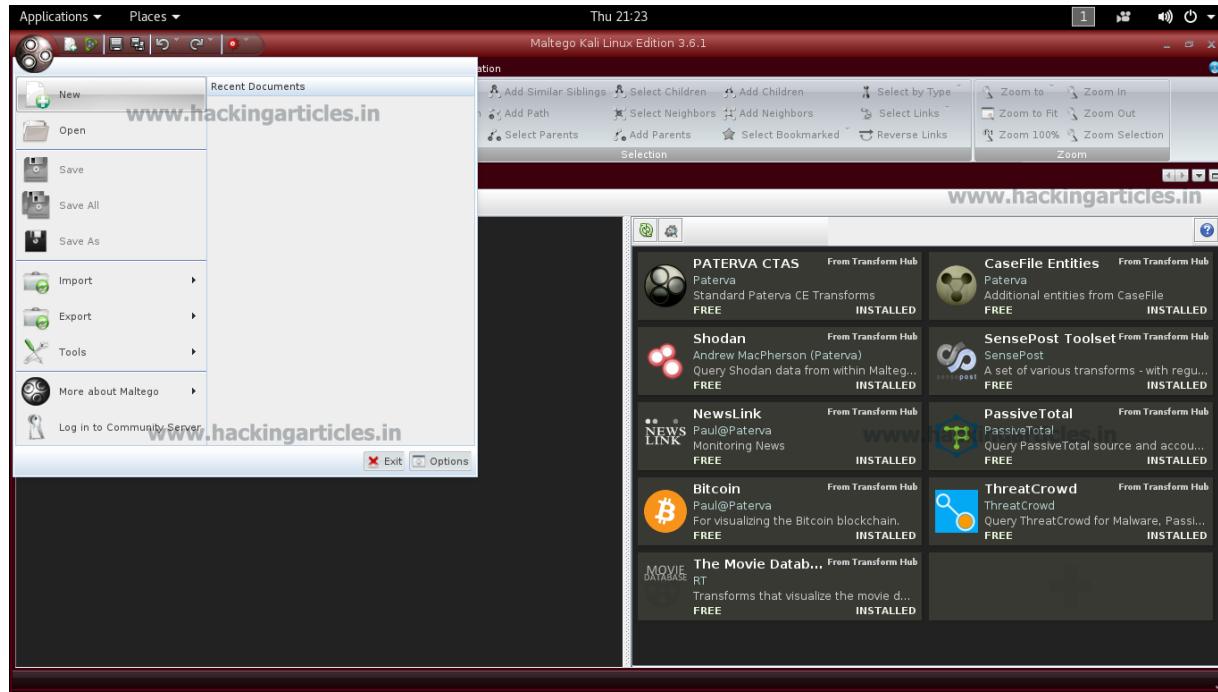




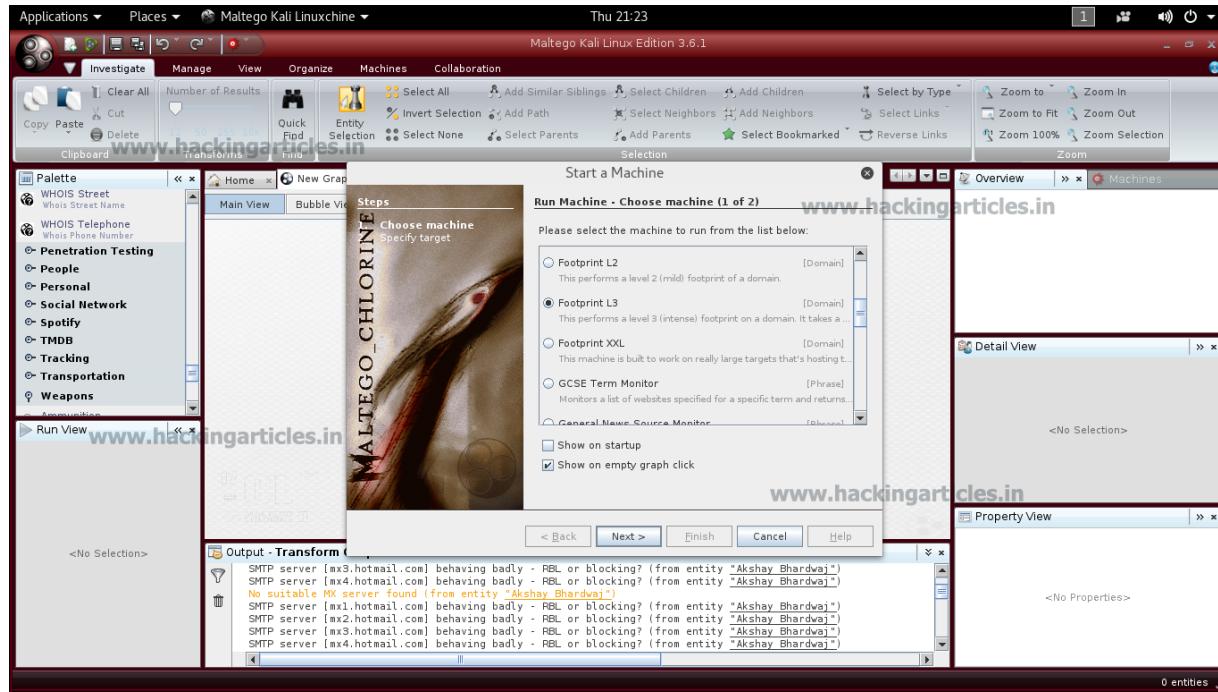
Now here you can see maltego's interface, and on the right side, there is few additional feature which you can install it to use in intense intelligence gathering they all require API's.



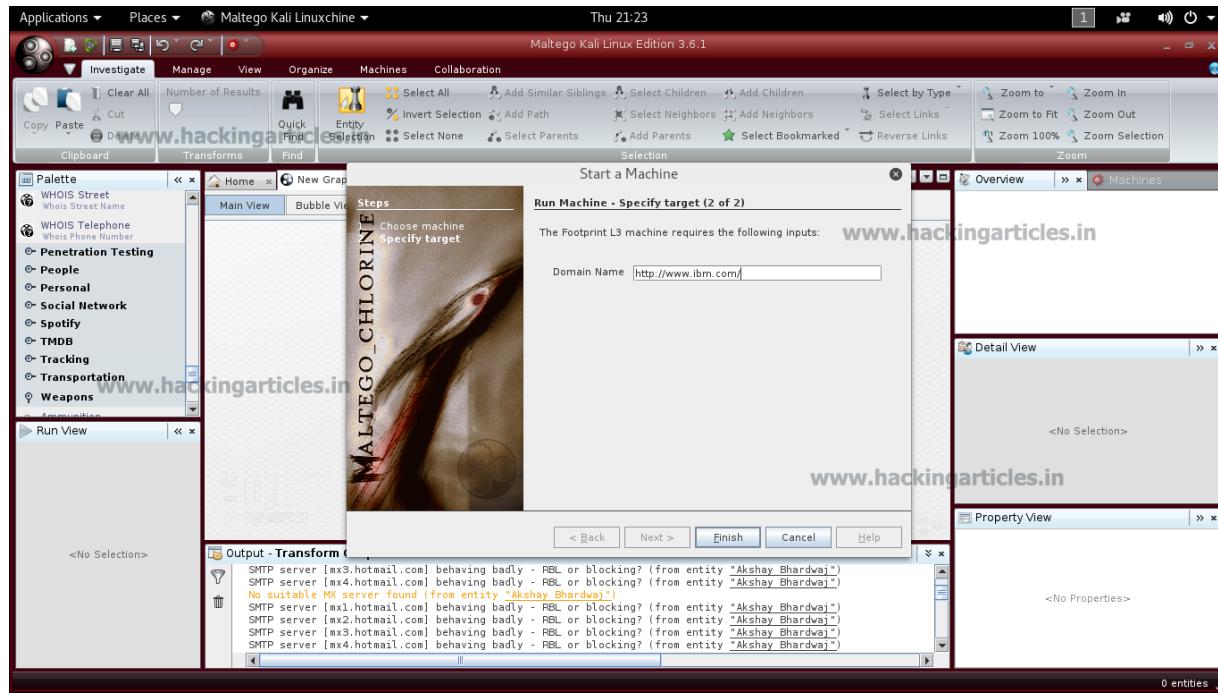
Now click on maltego icon and select new option to scan a new foot printing project.



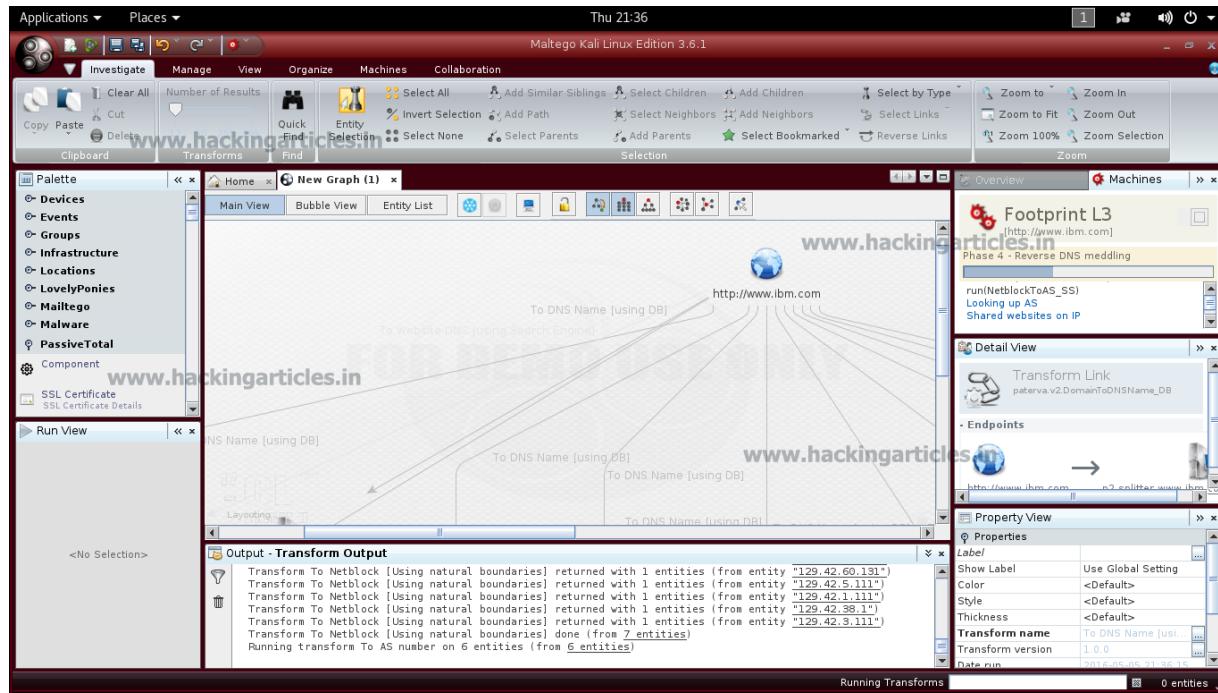
After that start a machine, here you can select the type of footprinting you want to perform there are many options here I select Footprint L3 and then click on next.

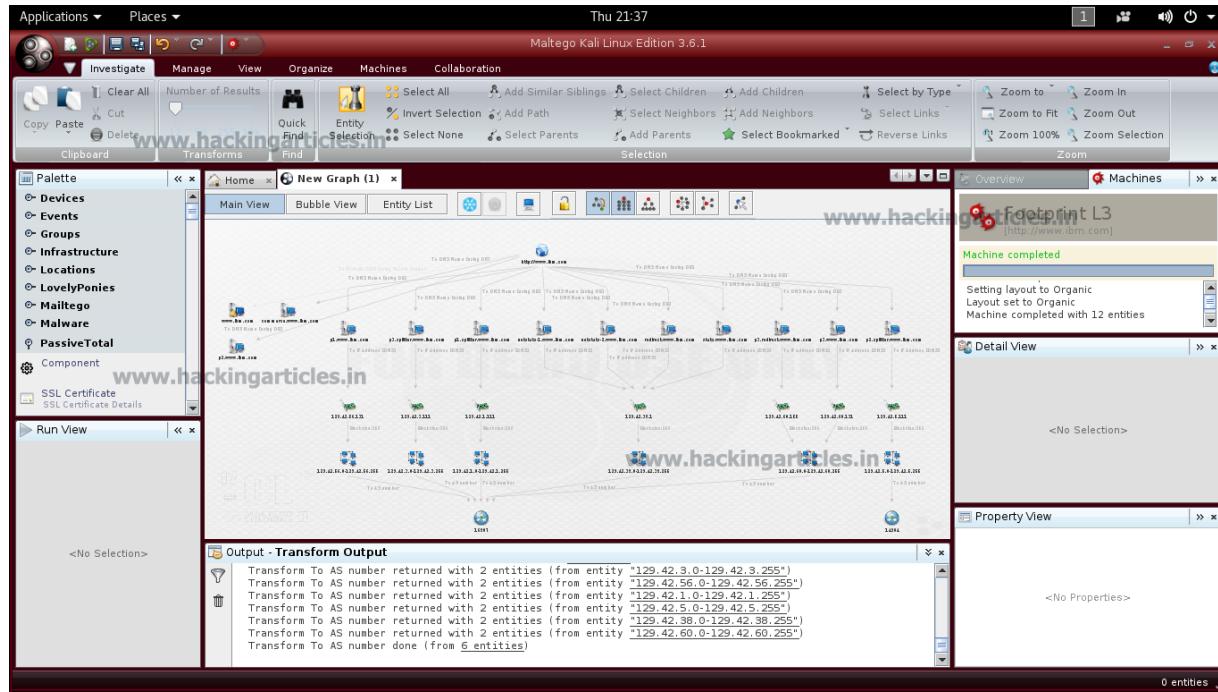


Now provide a Domain name and click on finish.

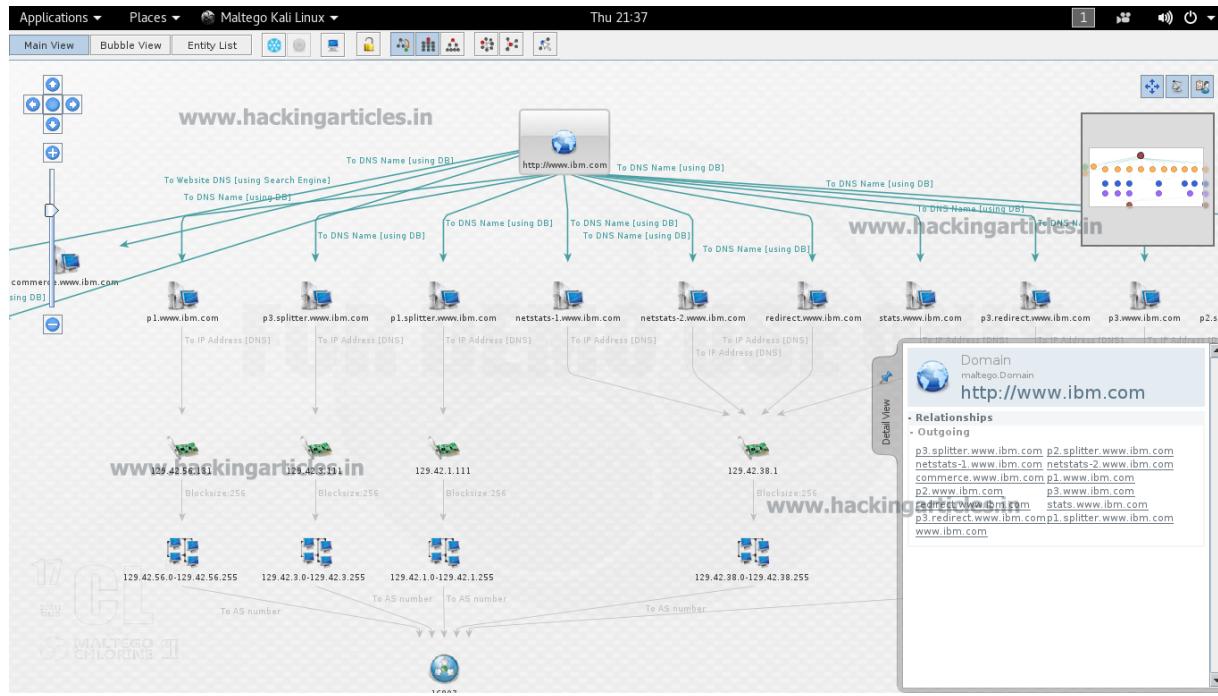


Now automatically maltego will start gathering information about the domain and create a graphical map of collected information.



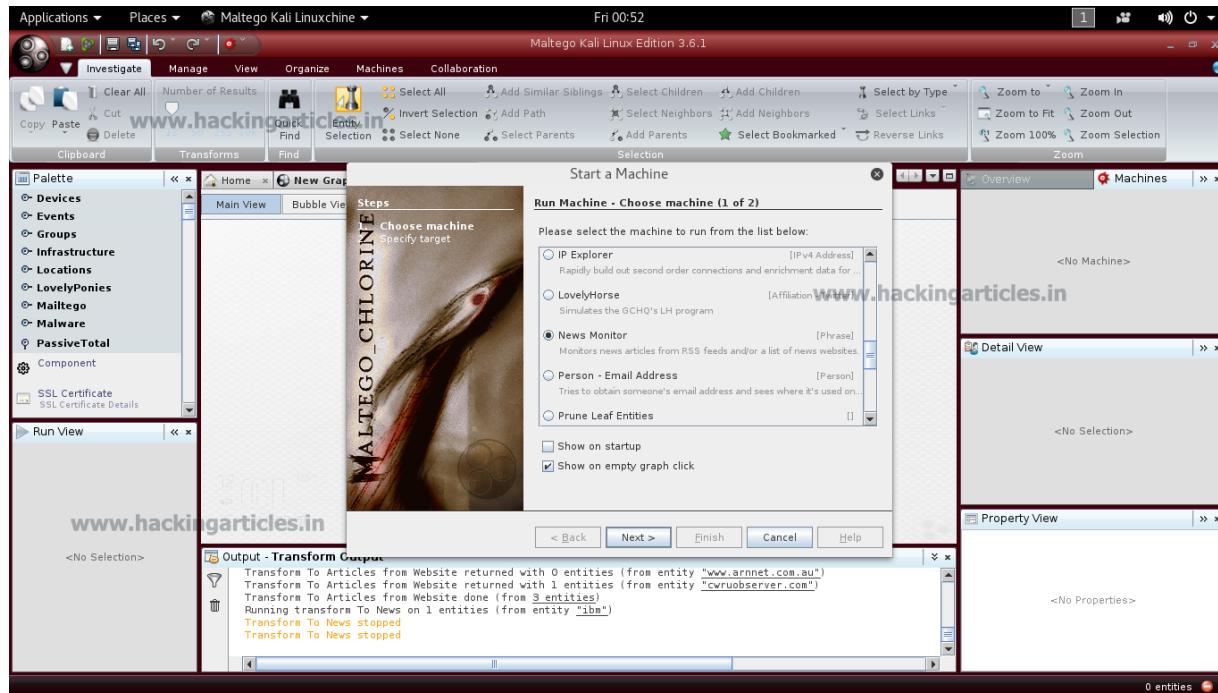


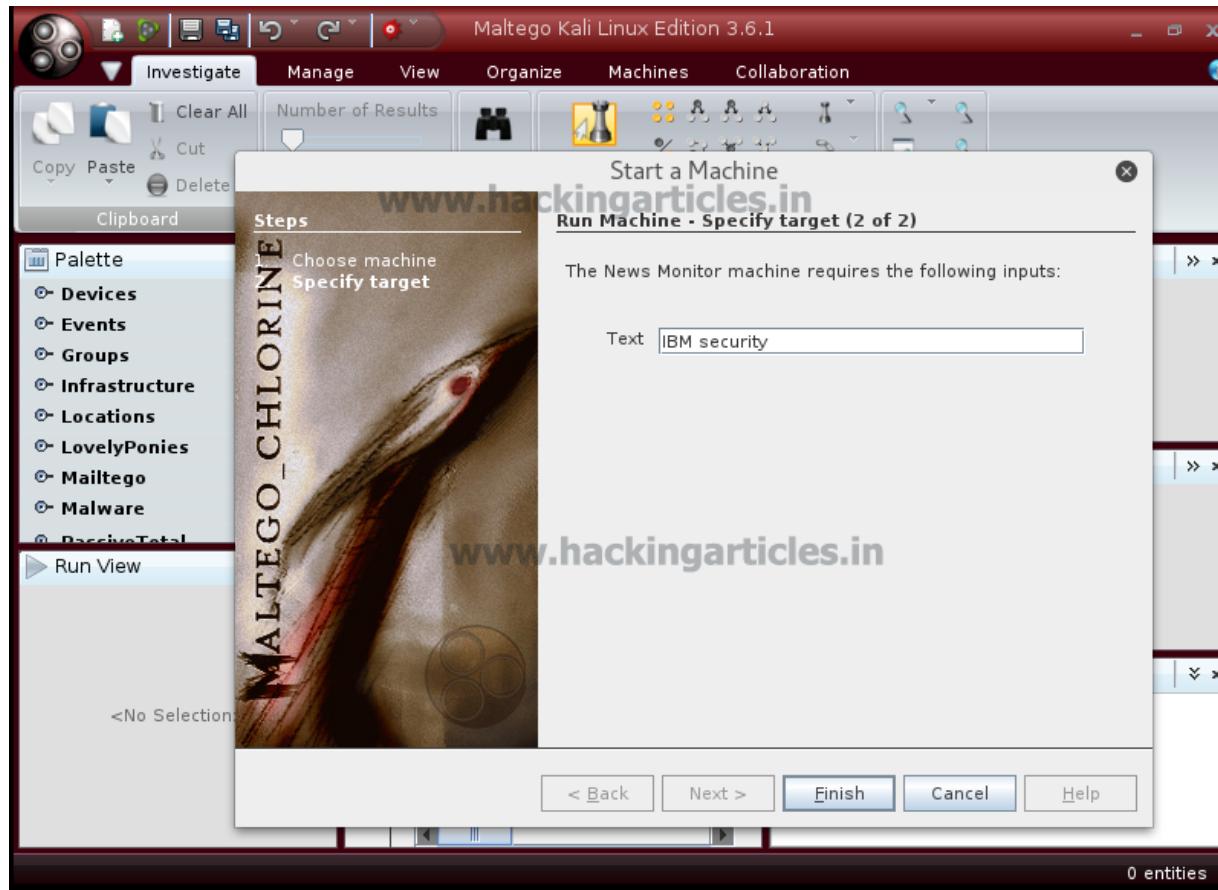
Now enlarge it to clearly view collected data. Here you can see ever information you need like DNS info, mail-server, IP, users, email-ID, connected computers, networks, etc.



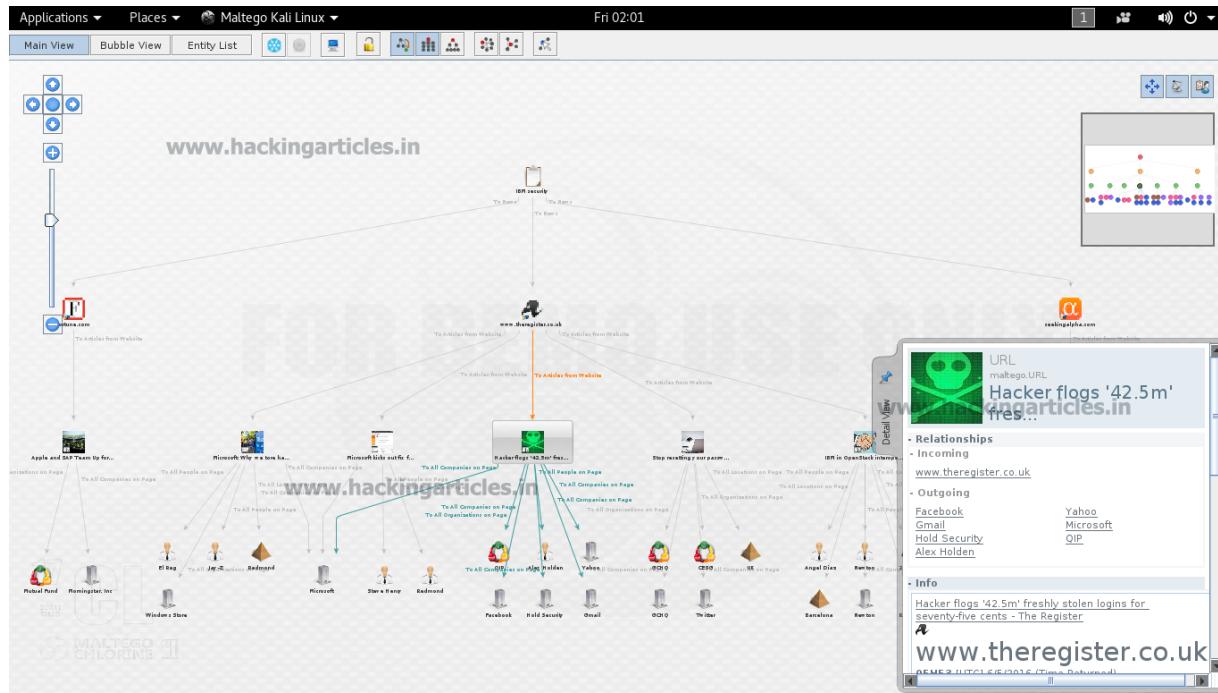
Now let's dig more about this domain, let's see what media or news publishers talking about this company.

Start a new machine and select News Monitoring click next and then type the keywords to know more about the company through online published articles.





And here you can see recently published articles about the company related to the keywords.



**Author:** AkshayBhardwaj is a passionate Hacker, Information Security Researcher | Sketch Artist | Technical writer. You can follow him on [LinkedIn](#) and [Facebook](#)

← OLDER POSTS