POST CATEGORY : Footprinting

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

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:

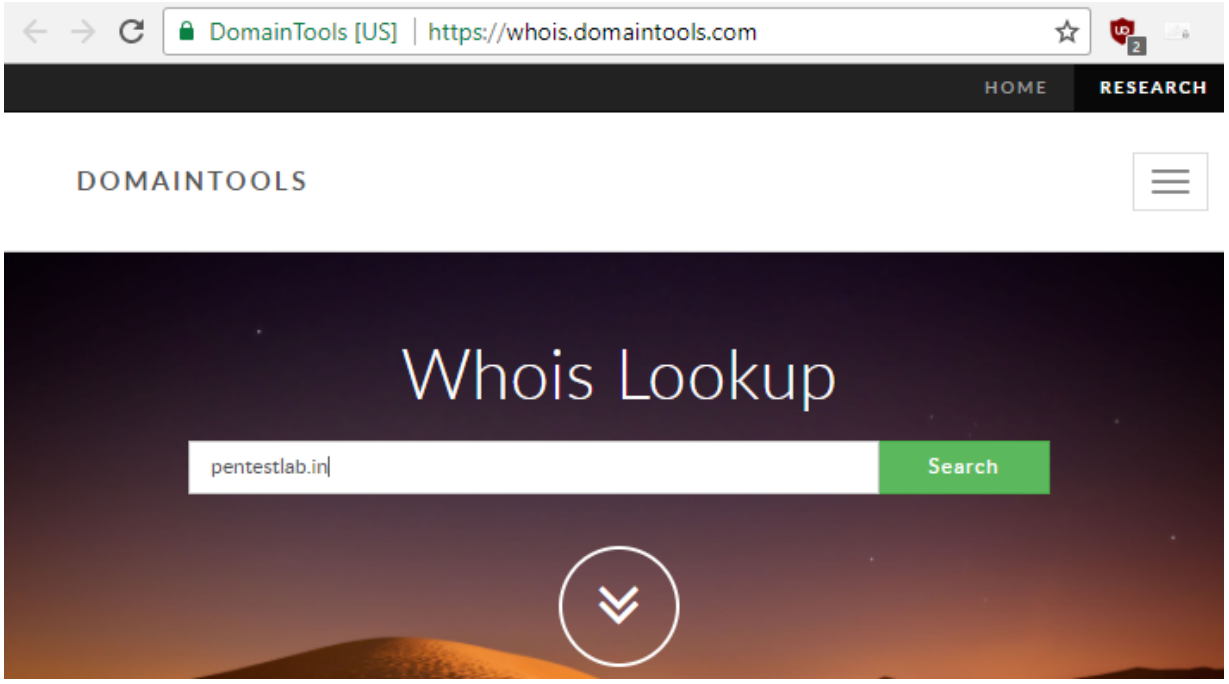
- Domain name details
- Contact details contain phone no. and email address of owner
- Registration date for domain name
- Expire date for domain name
- Domain name servers

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**

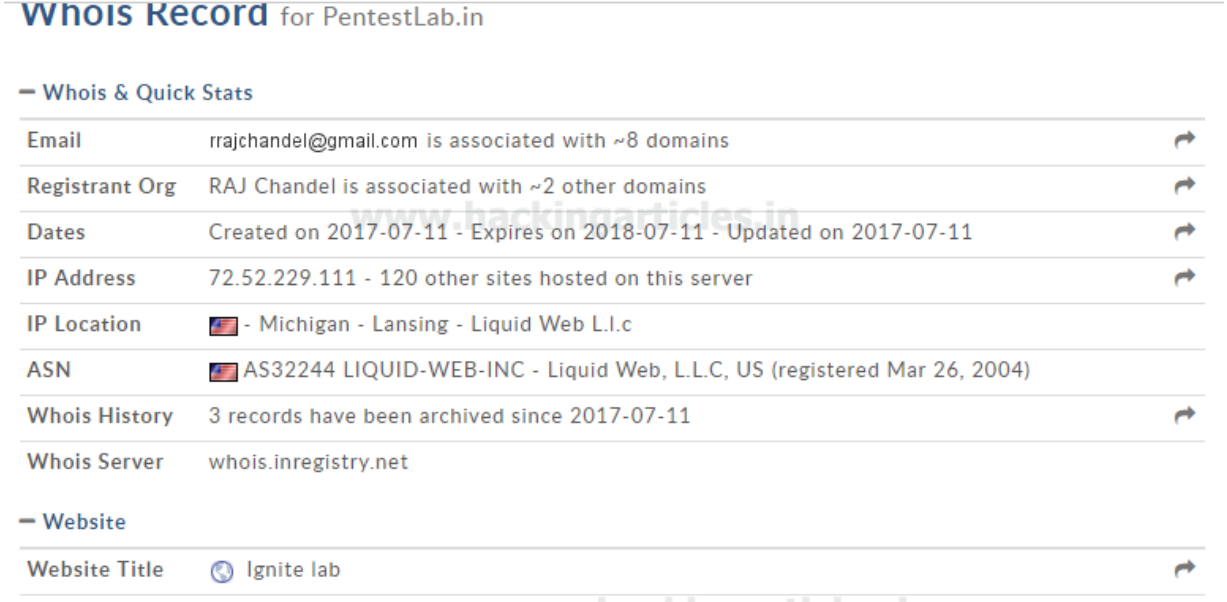


Now you can see it has created a whois record for pentestlab.in where it contains details like: **email address,IP, registrant Org**. From given record anyone can guess that this domain have some connection to raj chandel. Then attacker needs to perform footprinting on raj chandel taking help from previous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

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

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

Categories



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

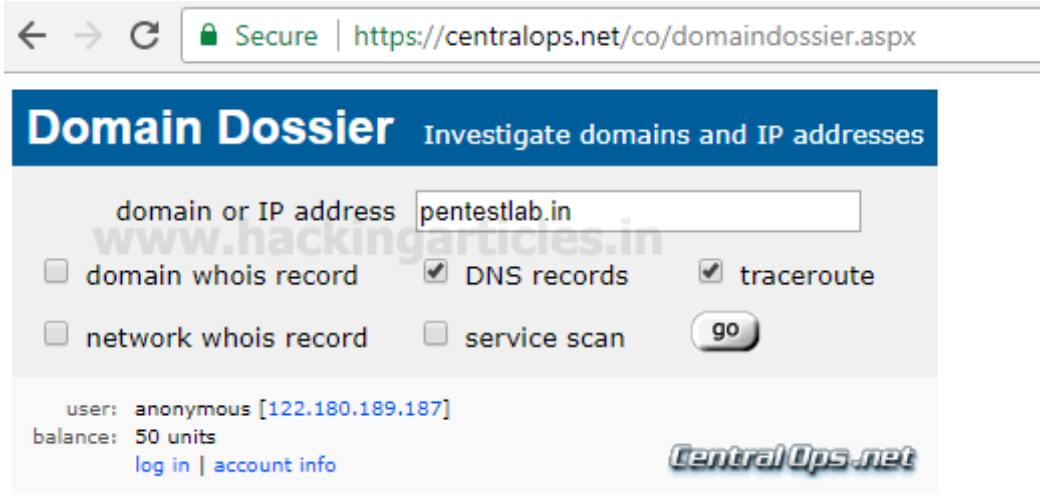
Facebook Page

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.**



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**and moreover details of DNS records TXT, SOA, NS, MX, A and PTR.

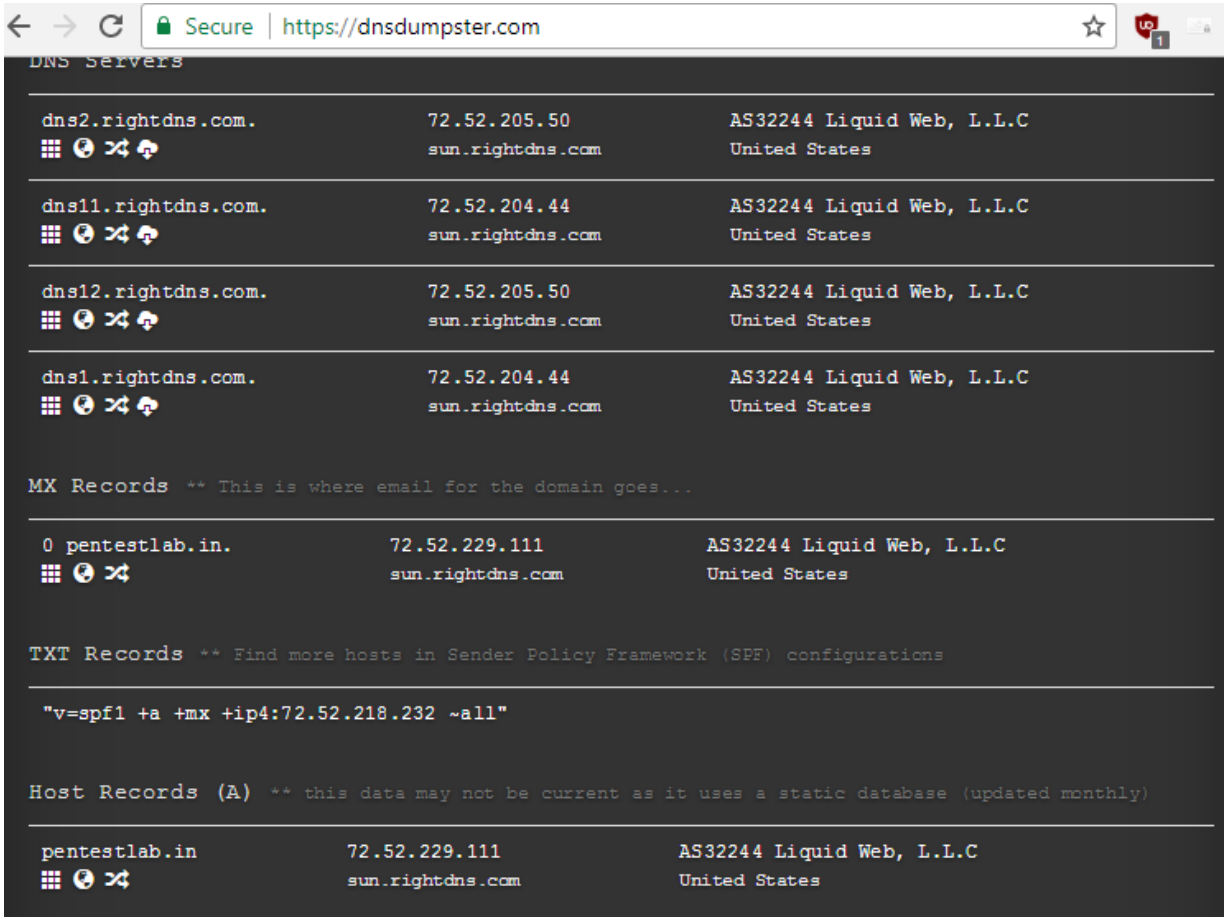
DNS records

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.



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.

Website Footprinting

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

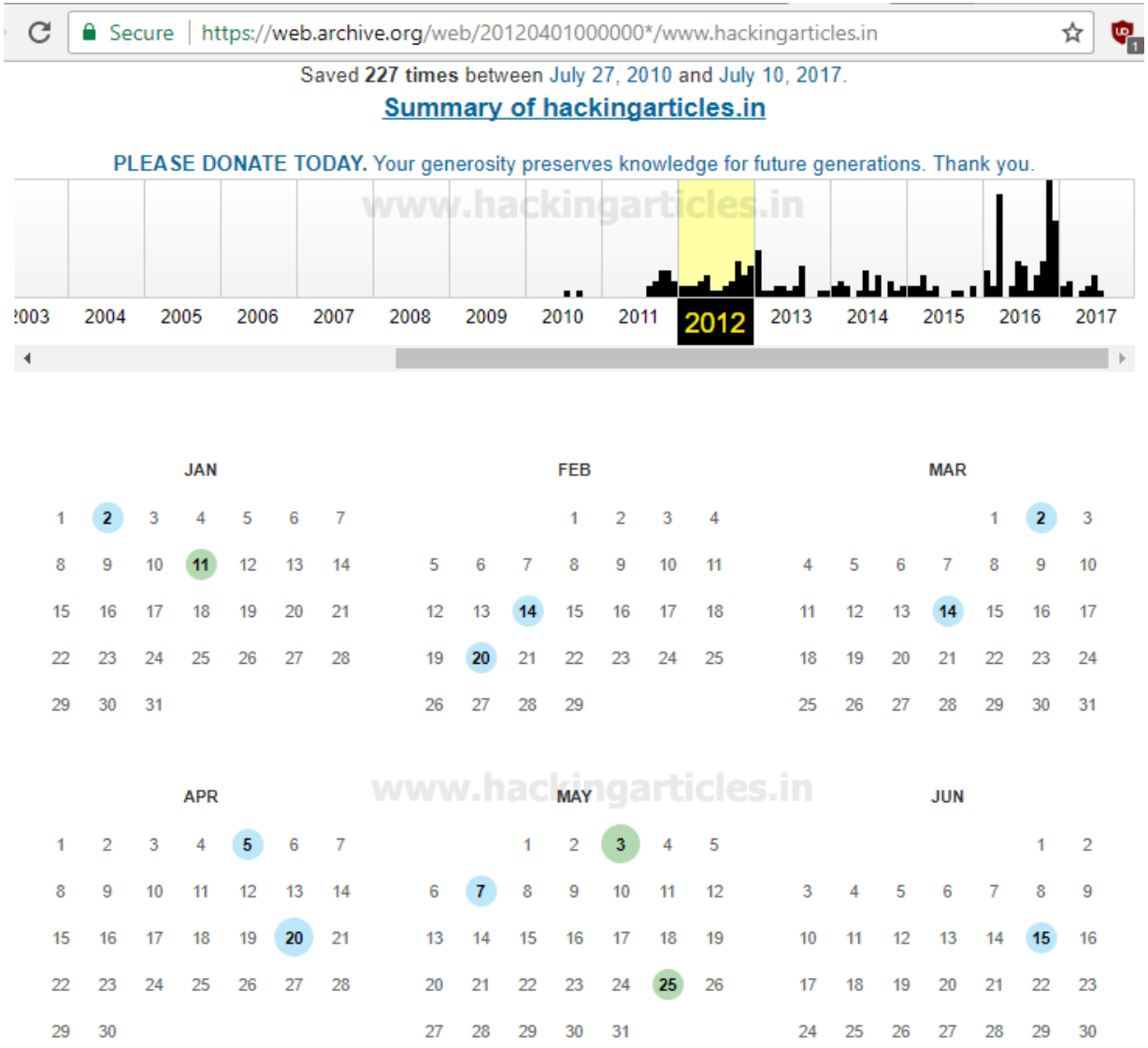
1. Archived description of website
2. Content management system and framework
3. Script and platform of the website and webserver
4. Web crawling
5. Extract meta data and contact details from website
6. Website and web page monitoring and analyzer

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** archived record of **2012.**

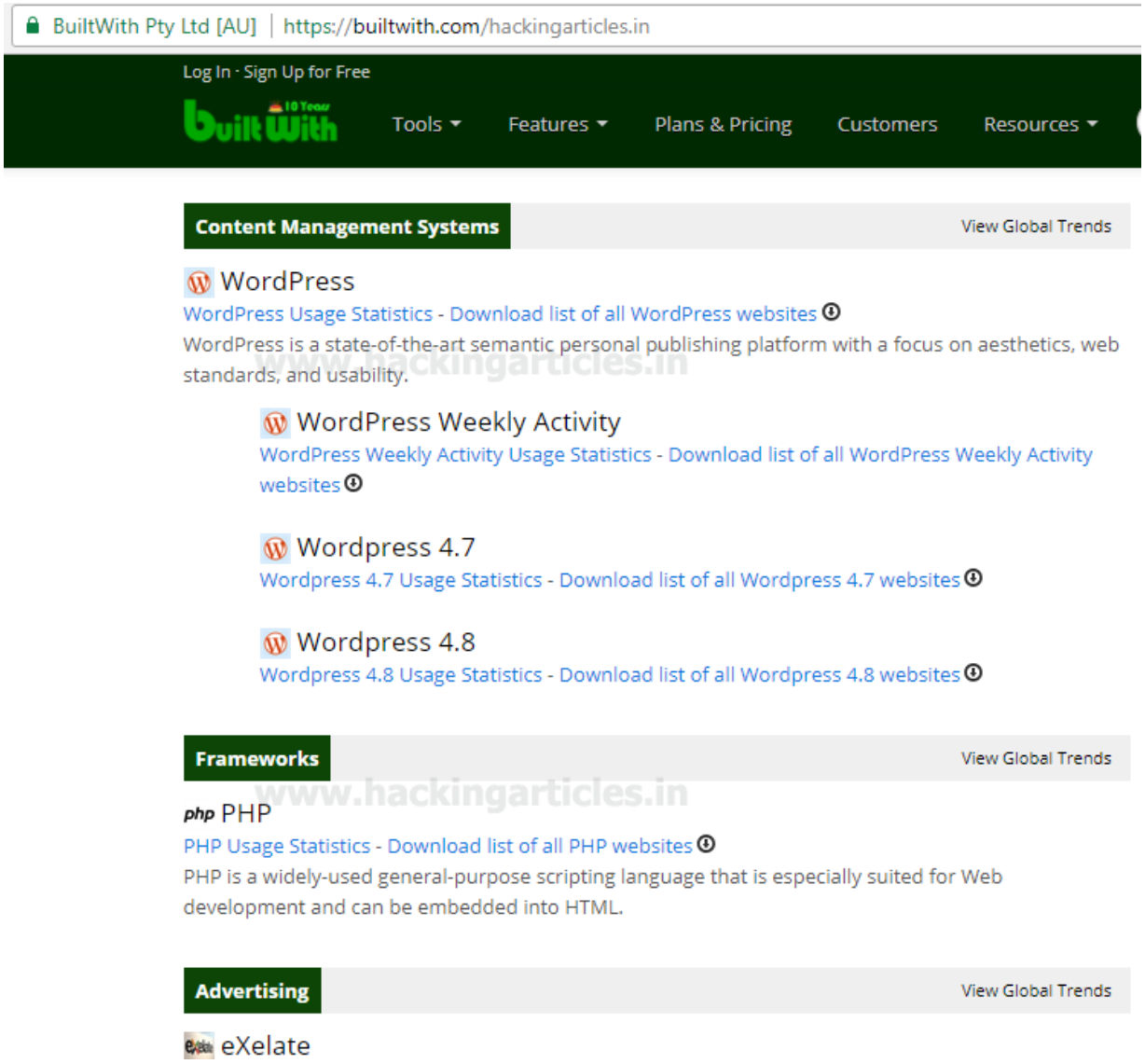


Built With: It is an online tool use for detecting techniques and framework involved inside running website.

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**



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

As result we receive same information as above

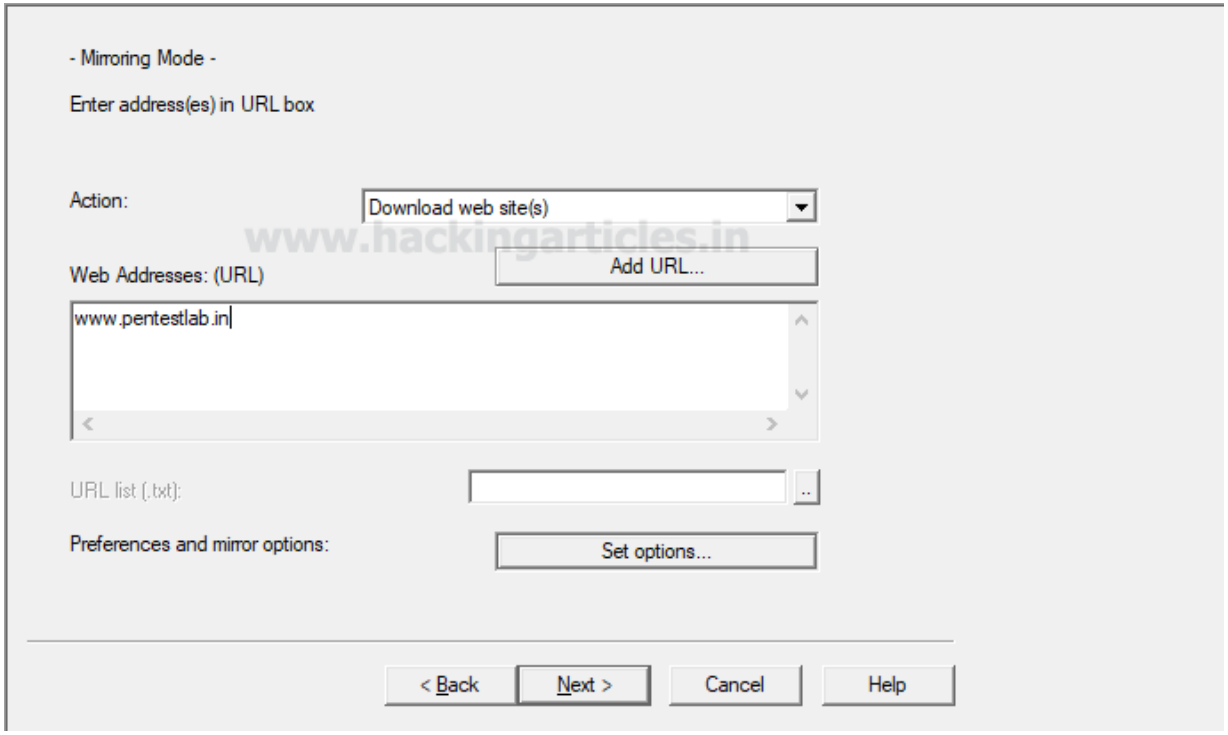
```
root@kali:~# whatweb www.pentestlab.in
http://www.pentestlab.in [200 OK] Apache, Country[UNITED STATES][US], HTML5, HTT
PServer[Apache], IP[72.52.229.111], JQuery, Script, Title[Ignite lab]
```

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 which starts downloading the website.

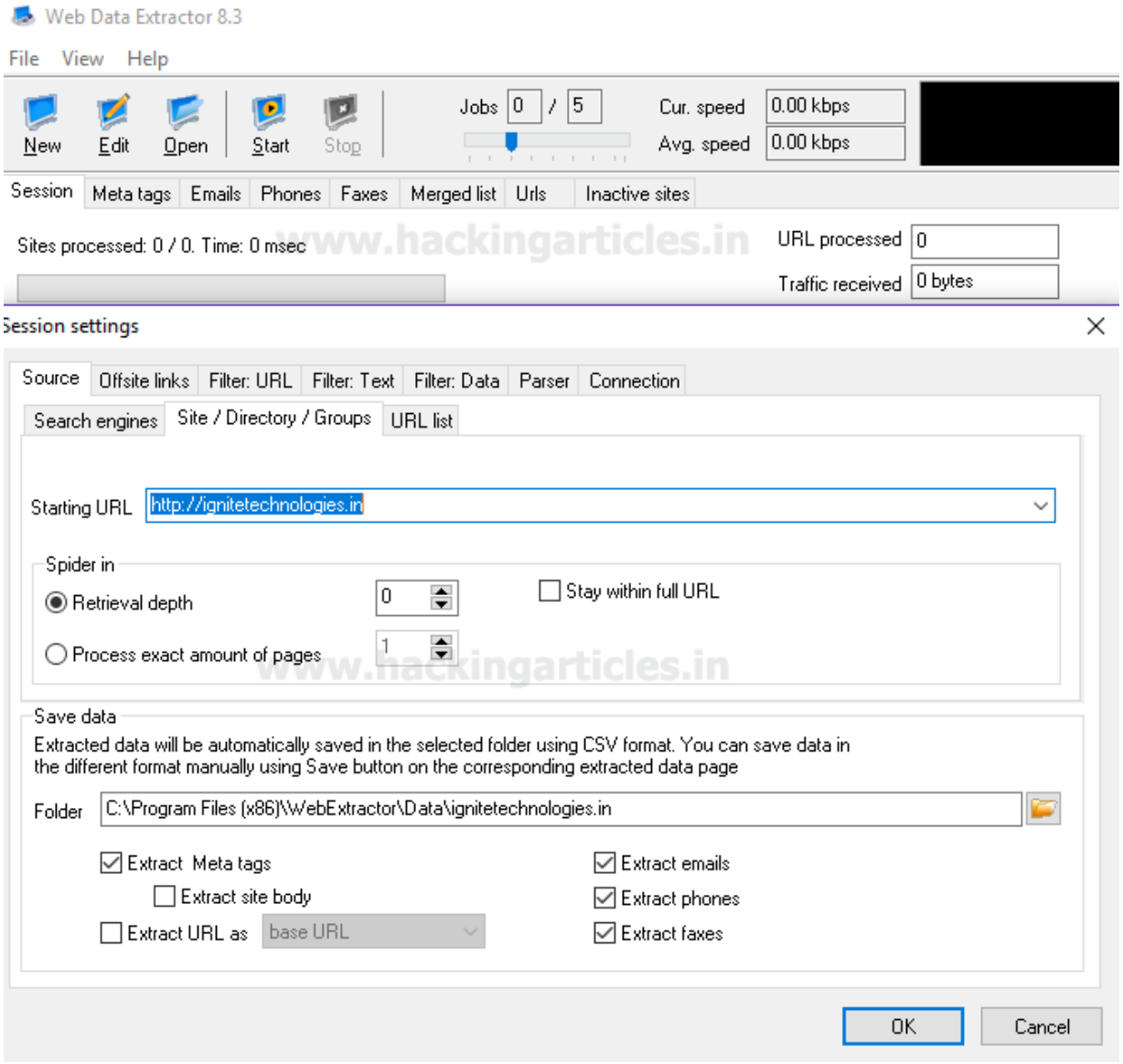


http://www.hackingarticles.in/5-ways-crawl-website/

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 ignitetechnologies.in and select folder to save the output and click on **ok.**

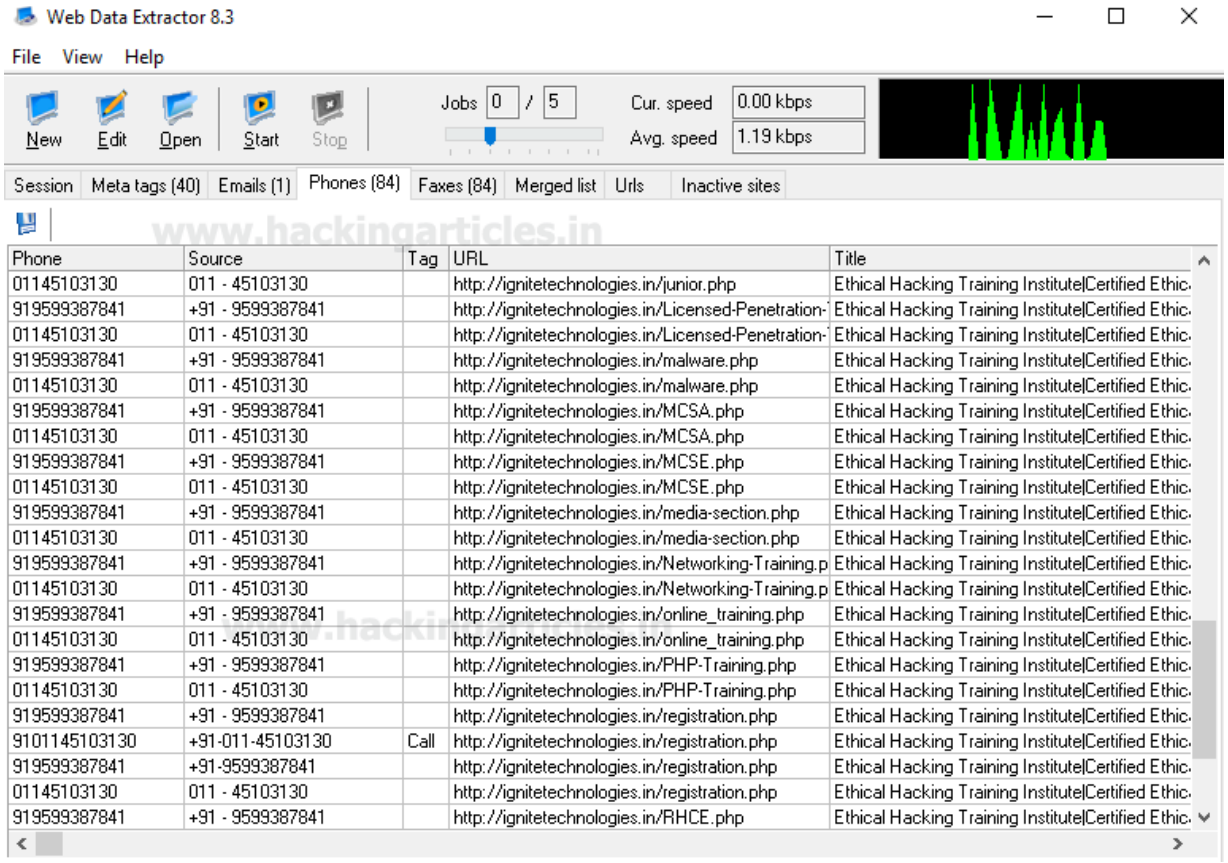


Now this tool will extract meta data, email contact no. and etc from inside the target URL.

From given screenshot you can see it found **40 meta tags1 email 84-phone number** from ignitetechnologies.in website.

Similarly there other tool use as web data extractor:

Web spider



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

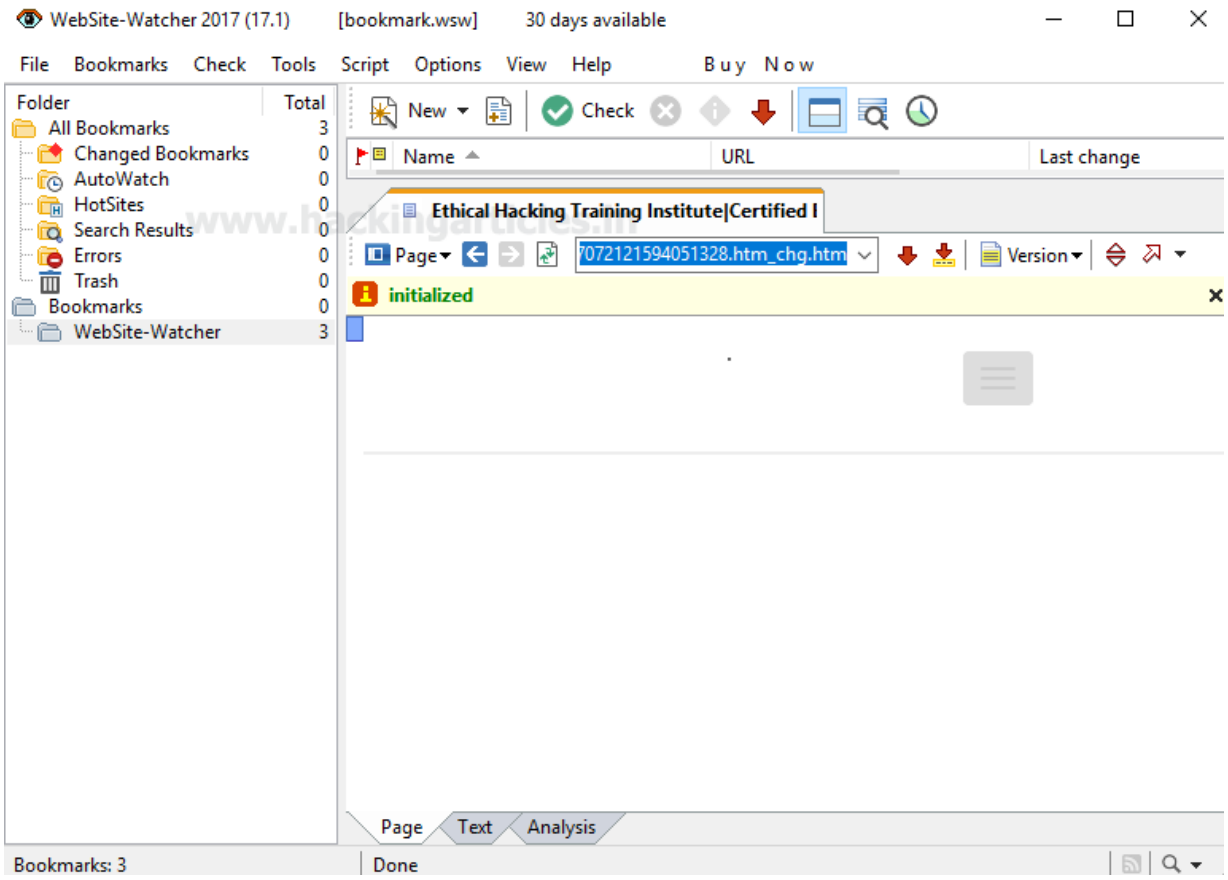
For example I enter URL hackingarticles.in for monitoring this website.

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

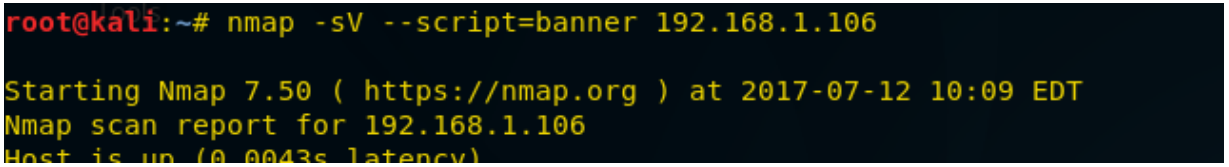
A simple banner grabber which connects to an open TCP port and prints out anything sent by the listening service within five seconds.

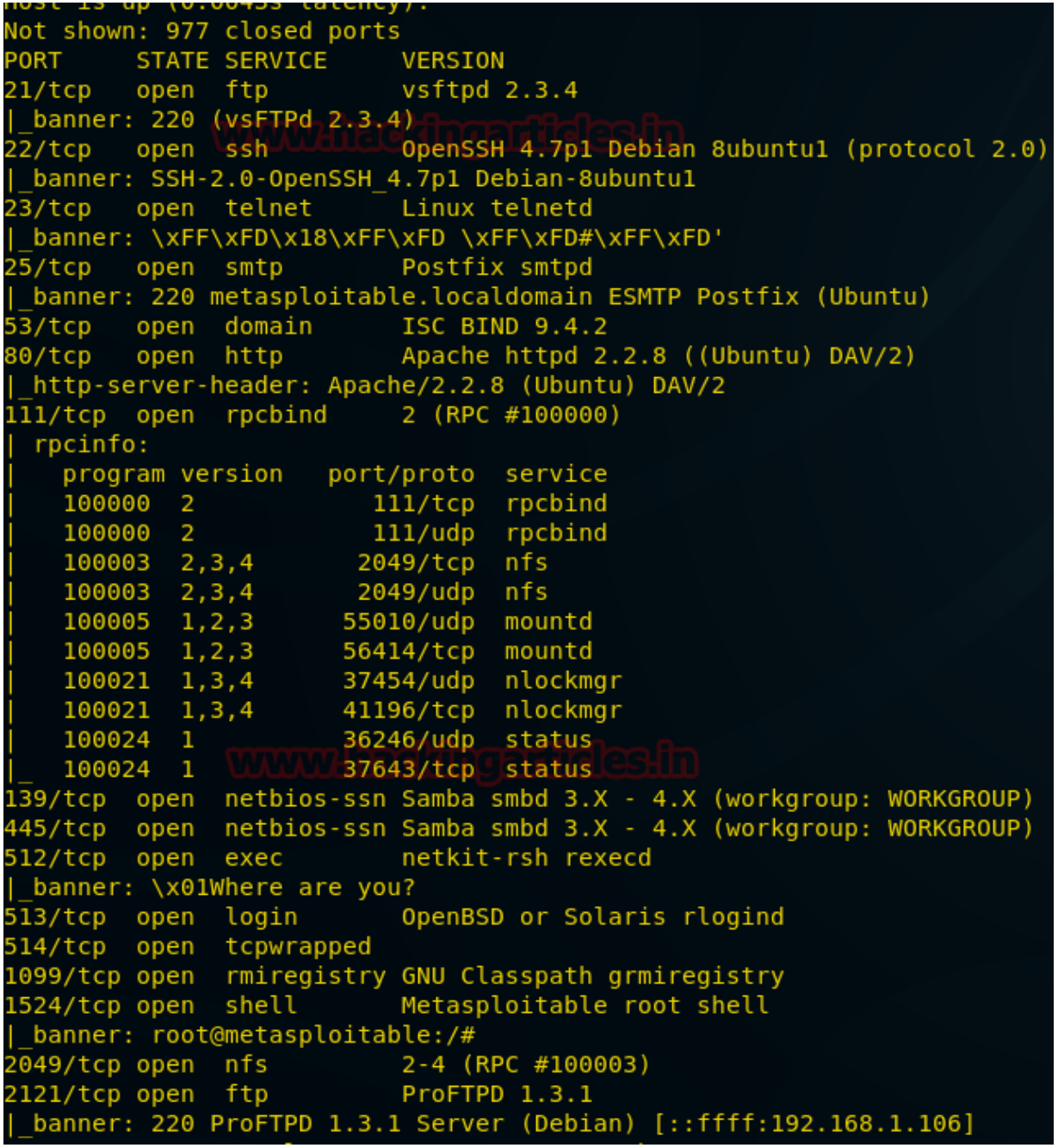
The banner will be shortened to fit into a single line, but an extra line may be printed for every increase in the level of verbosity requested on the command line.

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

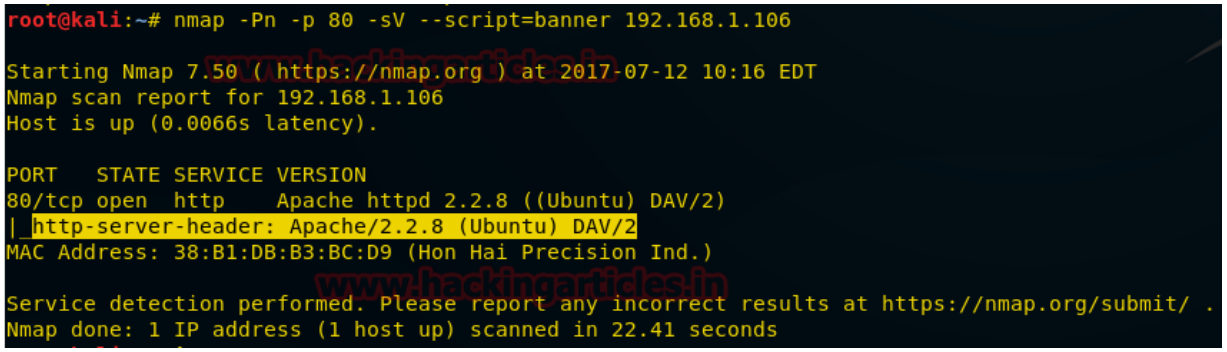




Following command will grab the banner for selected port i.e. **80** for http service and version.

```
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"



CURL

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

```
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"

Telnet

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

```
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
rying 192.168.1.106...
onnected to 192.168.1.106.
scape character is '^]'.
SH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

Netcat

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

```
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

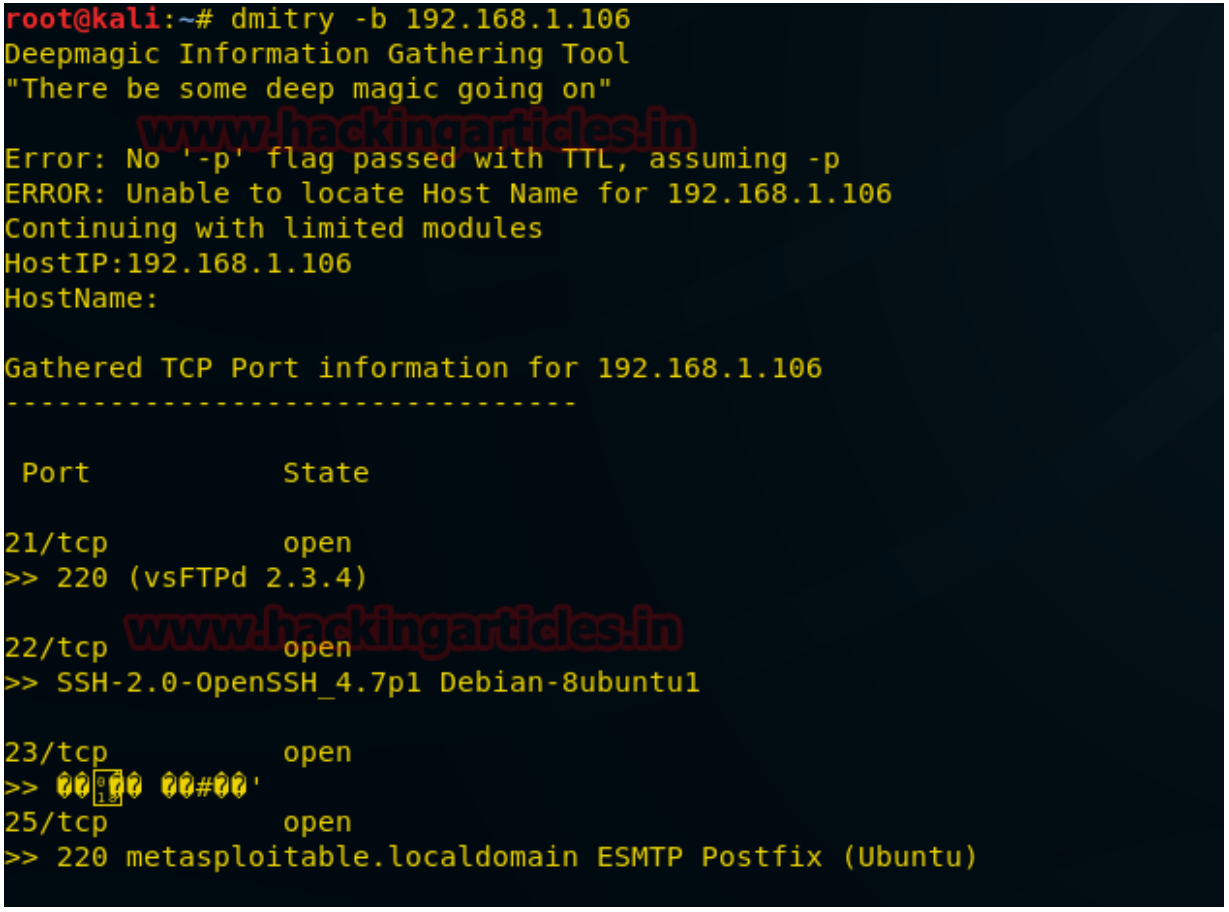
DMitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU)Linux Command Line Application coded in C. DMitry has the ability to gather as much information as possible about a host. Base functionality is able to gather possible subdomains, email addresses, uptime information, tcp port scan, whois lookups,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

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

```
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



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:

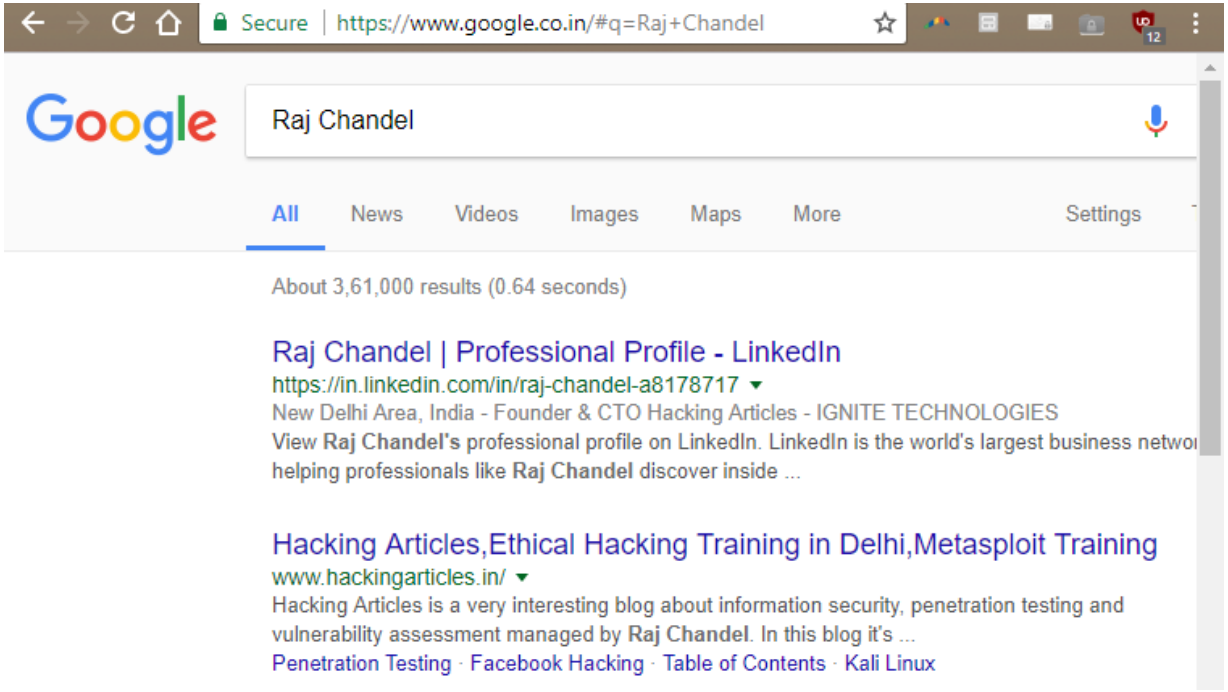
www.google.com

www.bing.com

www.shodan.io

www.duckduckgo.com

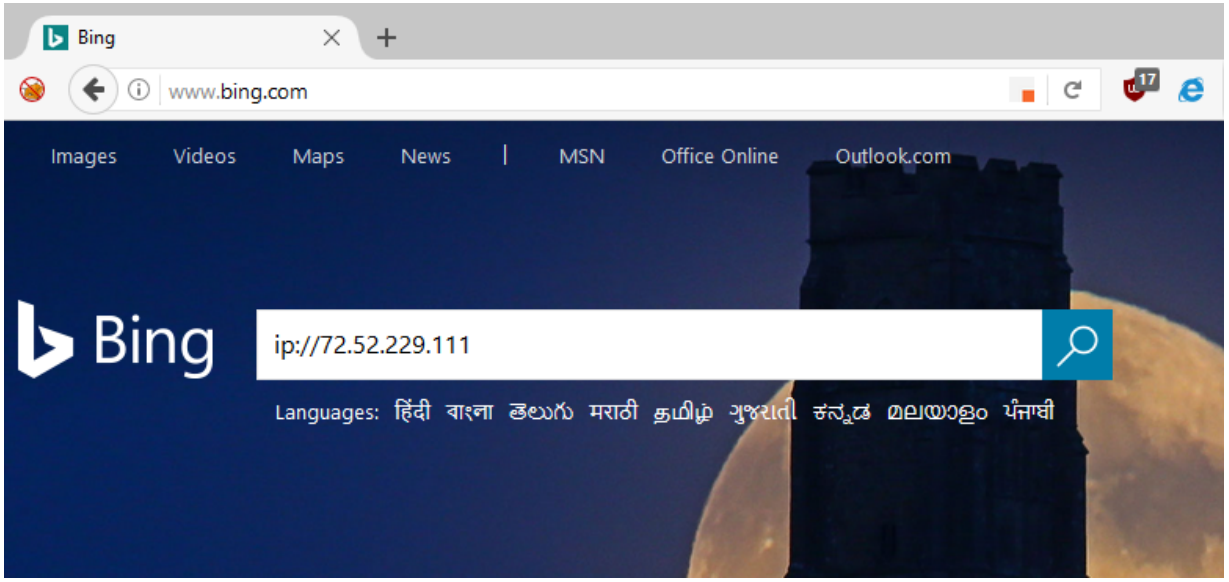
Now let's take example of google.com. If I search "Raj Chandel" in Google, then it will give me every possible result associated with the said person.



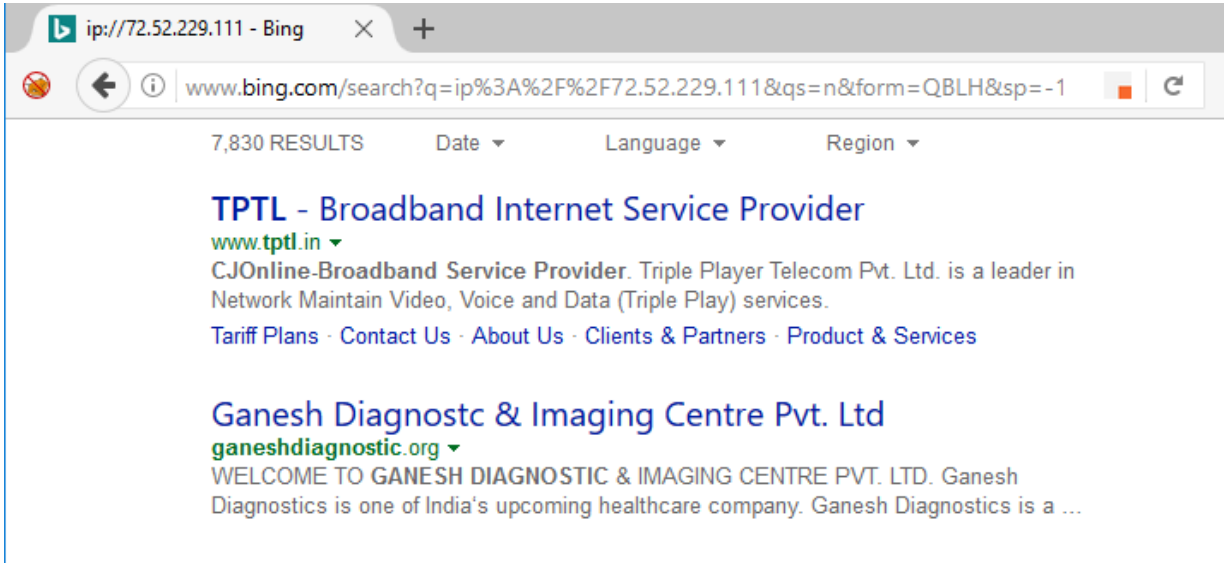
Same will be the result from other search engines. But different search engines are often used for particular searches. As shown above Google is good for general information. If you want to know that which websites are hosted on a particular server then you can use Bing search engine. To know an IP address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

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

Pinging ignitetechnologies.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
```

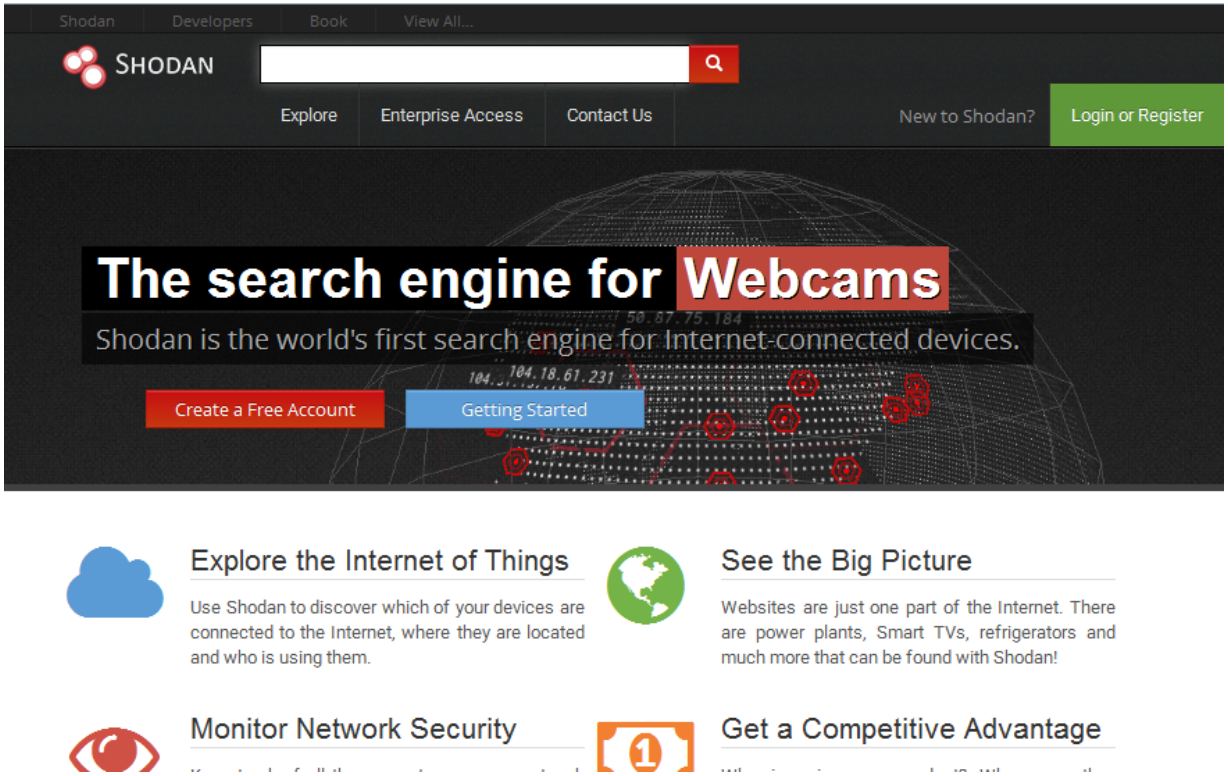
Now, open bing.com and type the IP in the search tab and press enter.



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



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.



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.careerbuilder.co.in/

www.dice.com

www.simplyhired.com

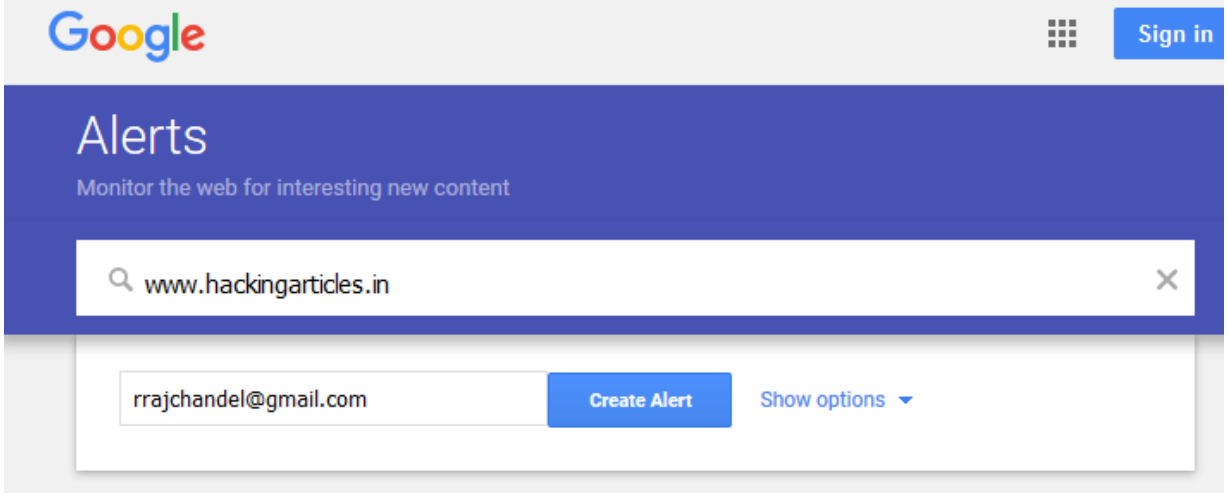
www.indeed.com

www.usajobs.gov

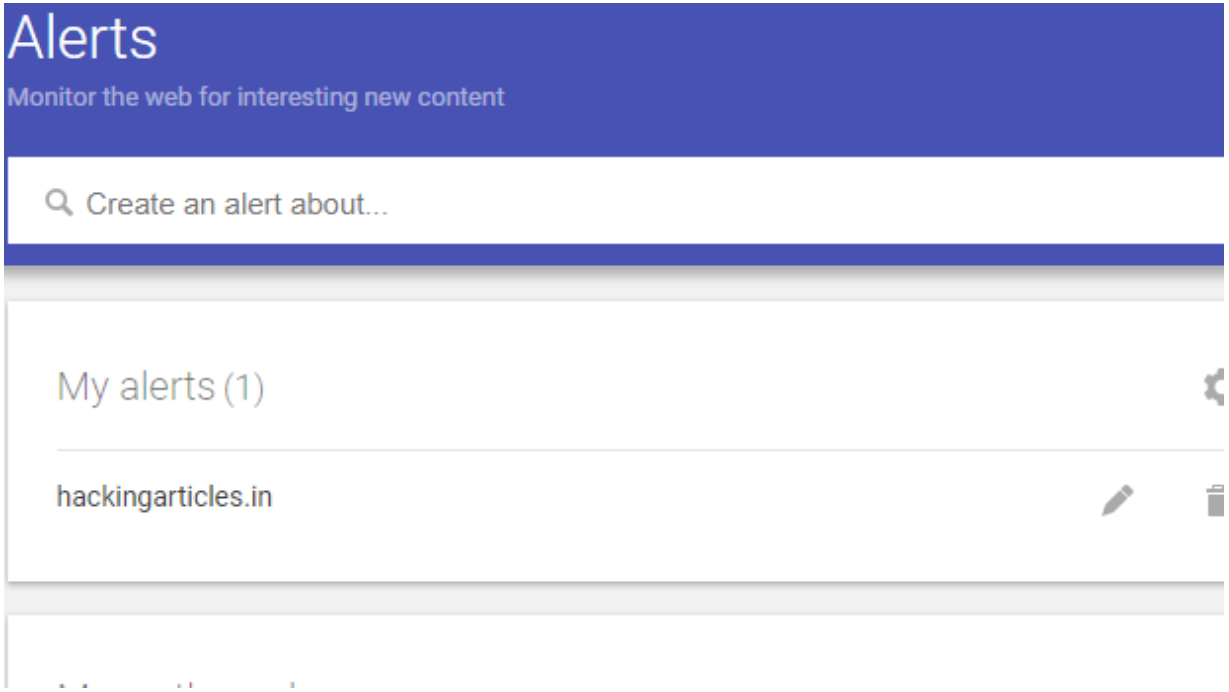
www.naukri.com

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 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.



Footprinting through Social Networking sites

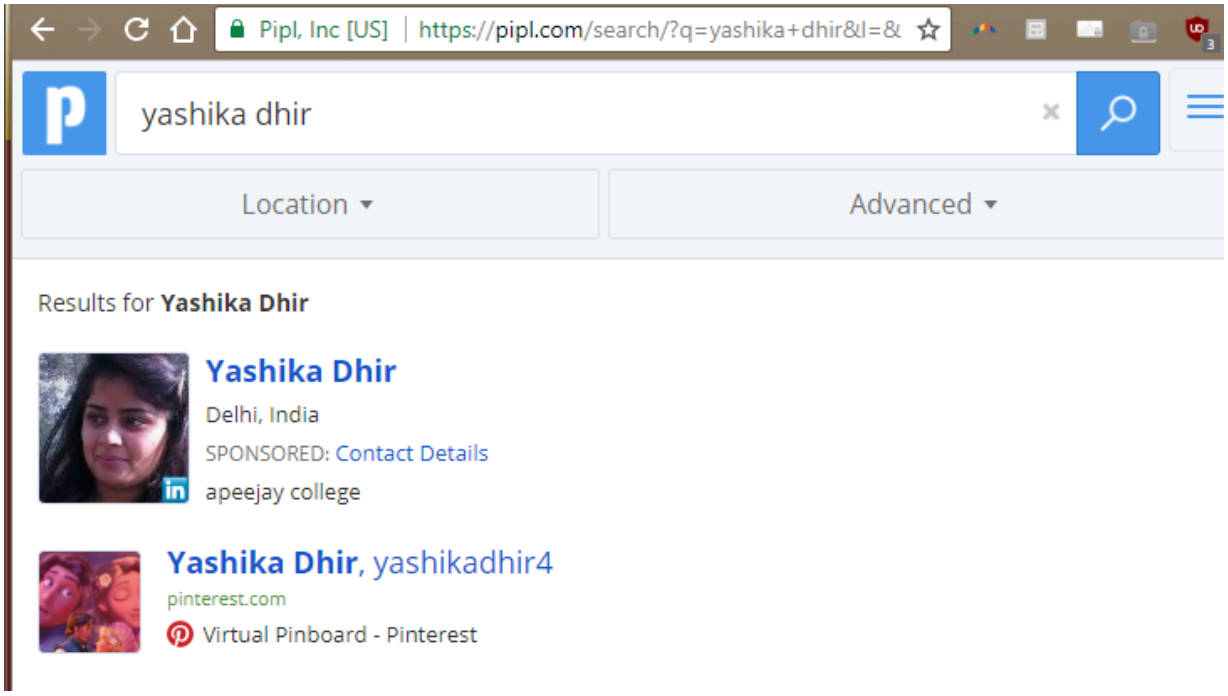
Attackers use social networking sites like Facebook, Twitter, and Pinterest etc. to gain important and sensitive data about their target. They often create fake profiles through these social media to lure their target and extract vulnerable information.

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.

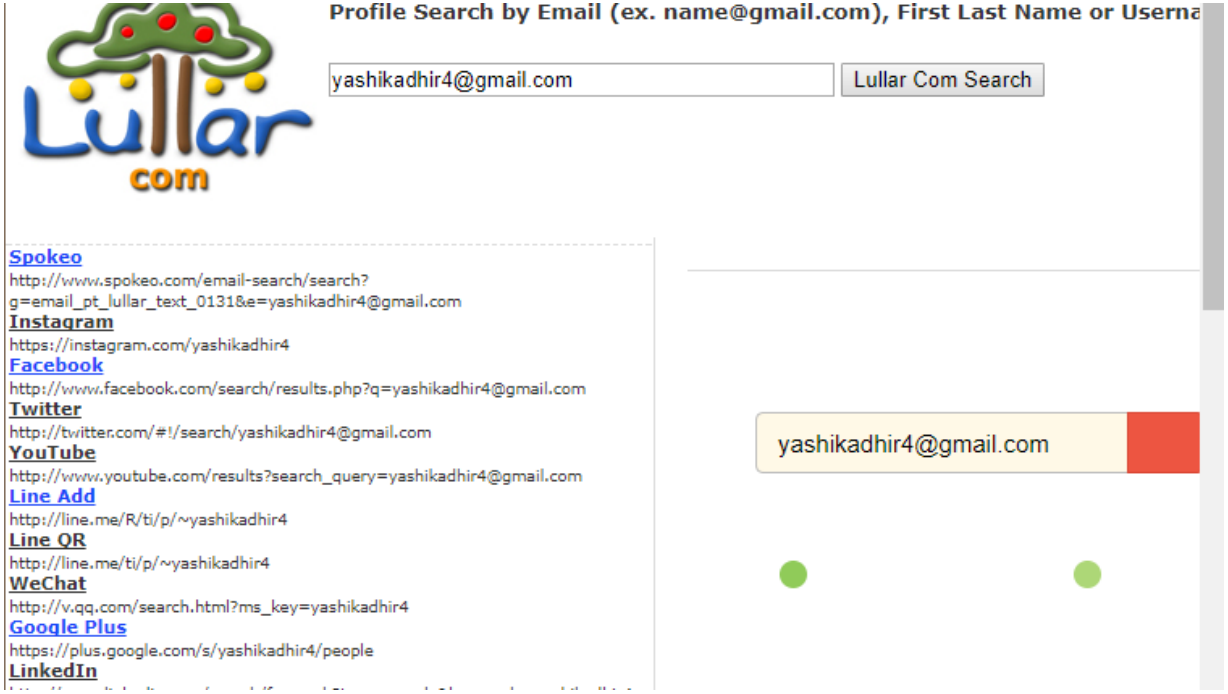
Even the information about the employee's interest is tracked and then they are trick into revealing more information.

Now if you want to search particular person using just their name or email then there are specialized websites for it like pipl.com and lullar.com

Open 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.



Now open 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.



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~~

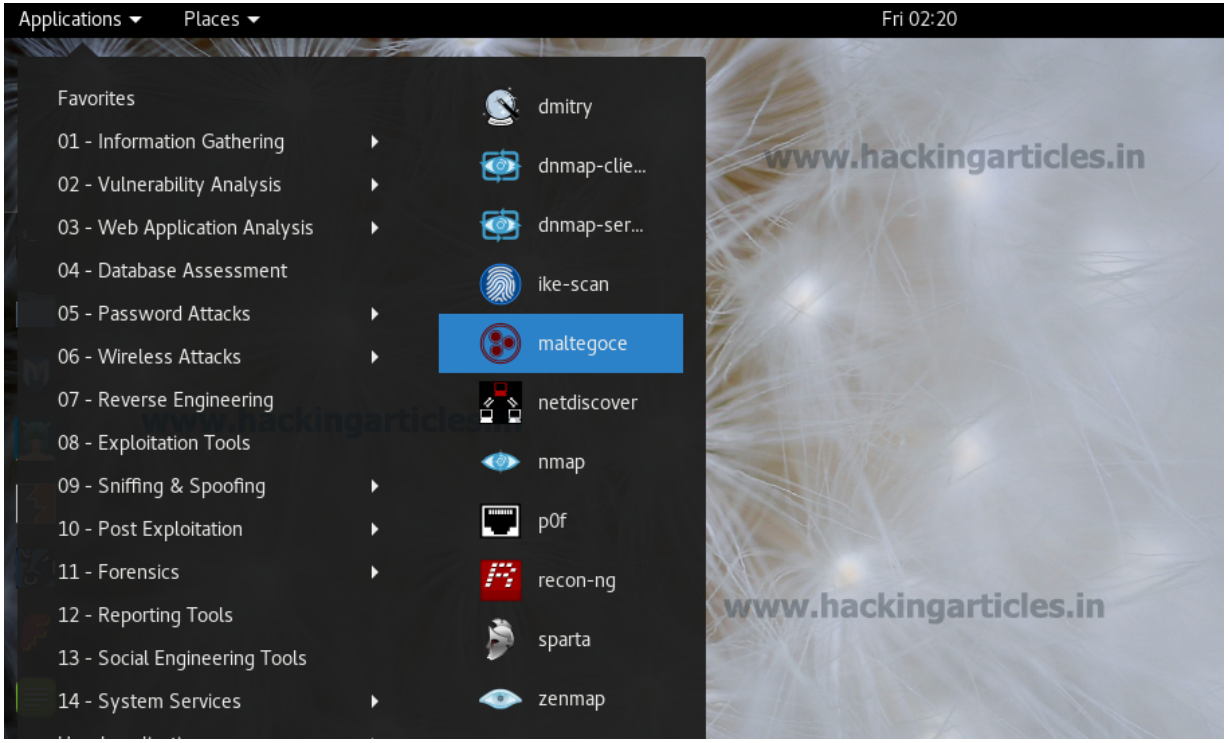
Information Gathering using Maltego (Beginner Guide)

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.

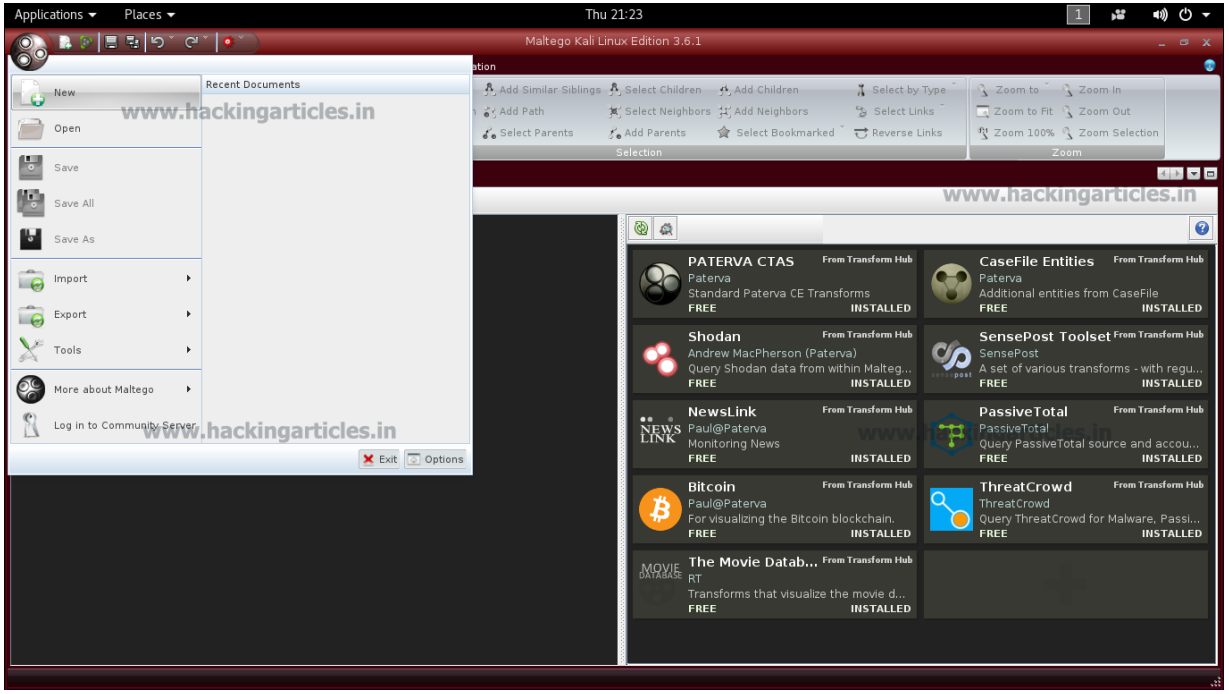
So, let's see how to use it for intelligence gathering.

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

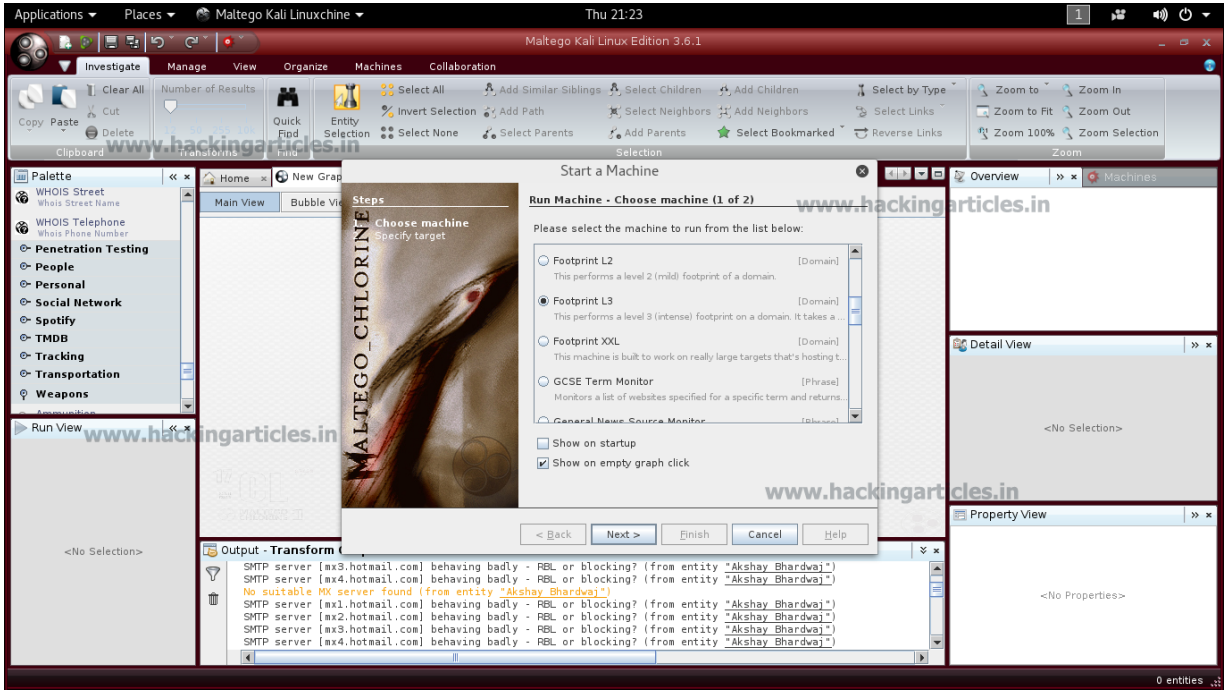


Now here you can see maltego's interface, and on the right side, there is few additional feature which you can install it to use in intense intelligence gathering they all require API's.

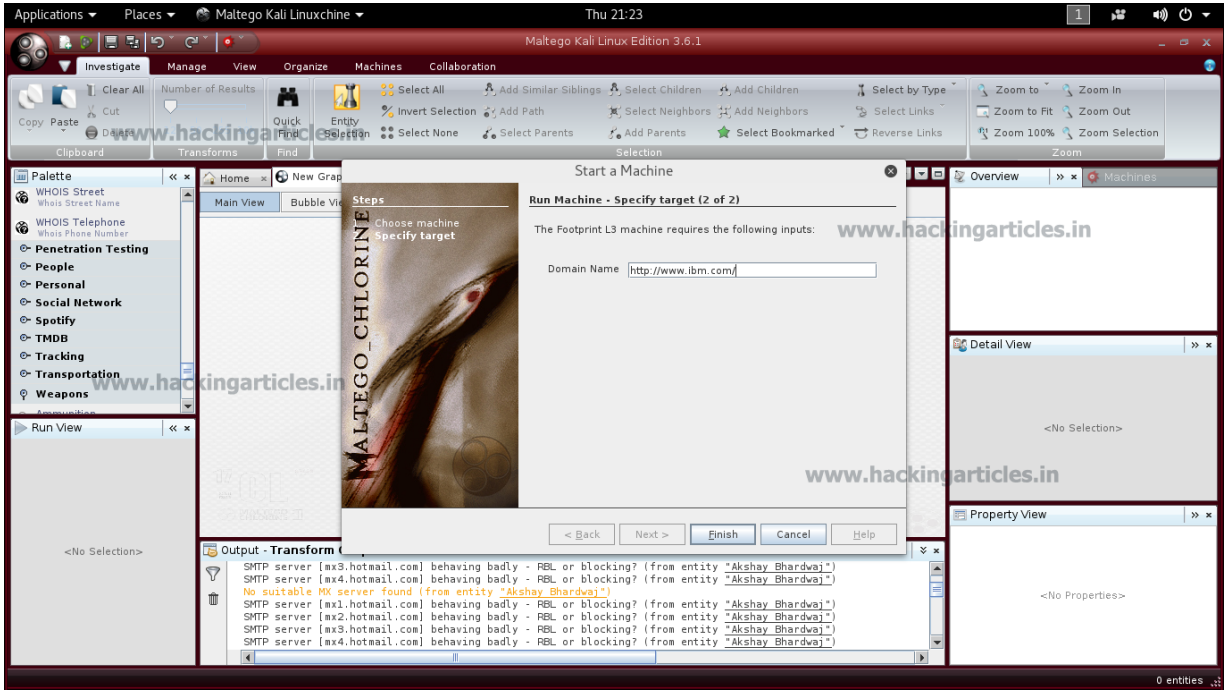
Now click on maltego icon and select **new** option to scan a new foot printing project.



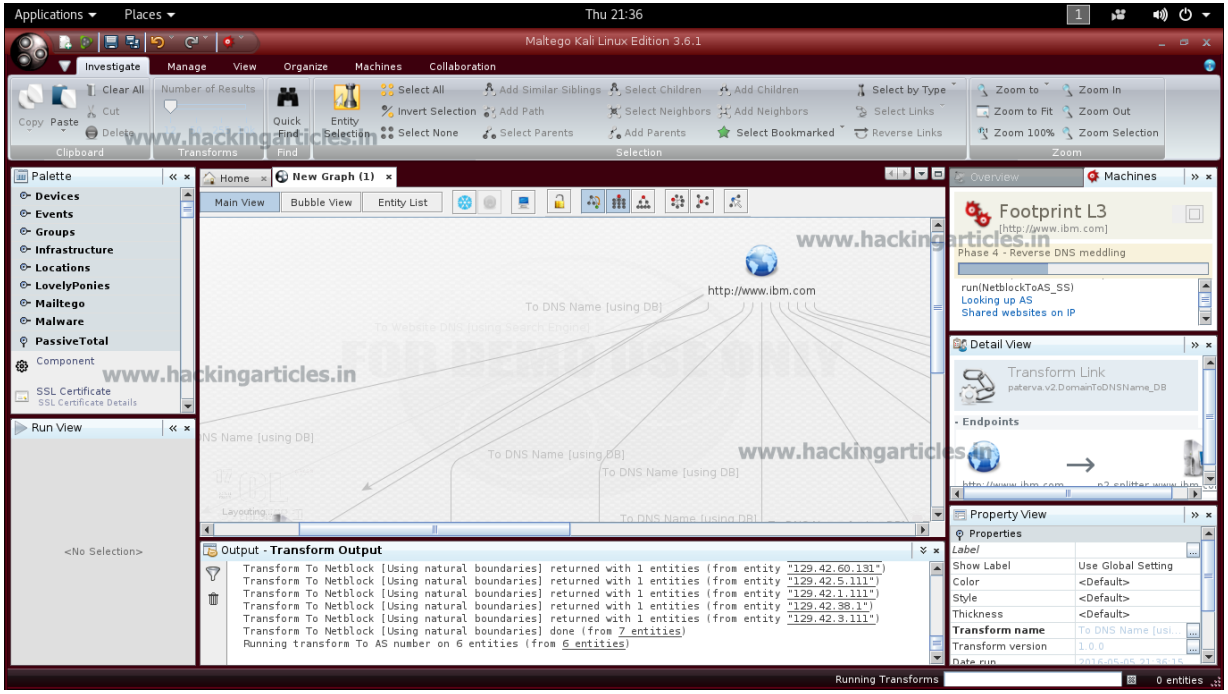
After that start a machine, here you can select the type of footprinting you want to perform there are many options here I select Footprint L3 and then click on next.

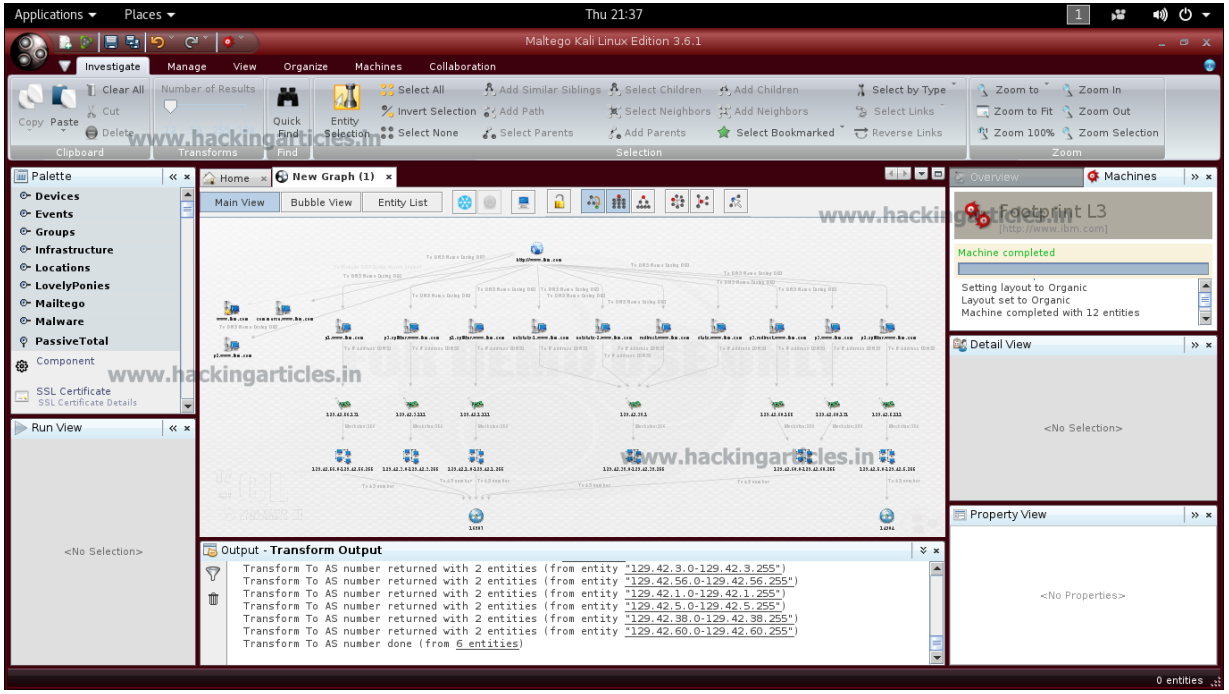


Now provide a Domain name and click on finish.

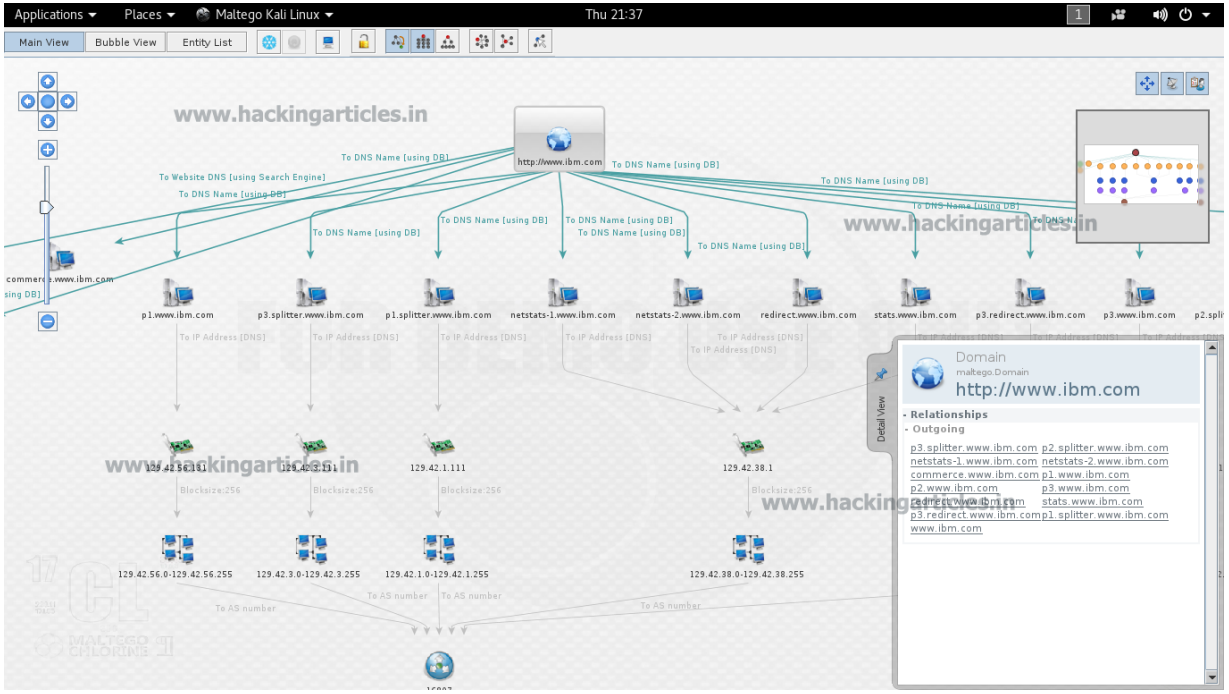


Now automatically maltego will start gathering information about the domain and create a graphical map of collected information.



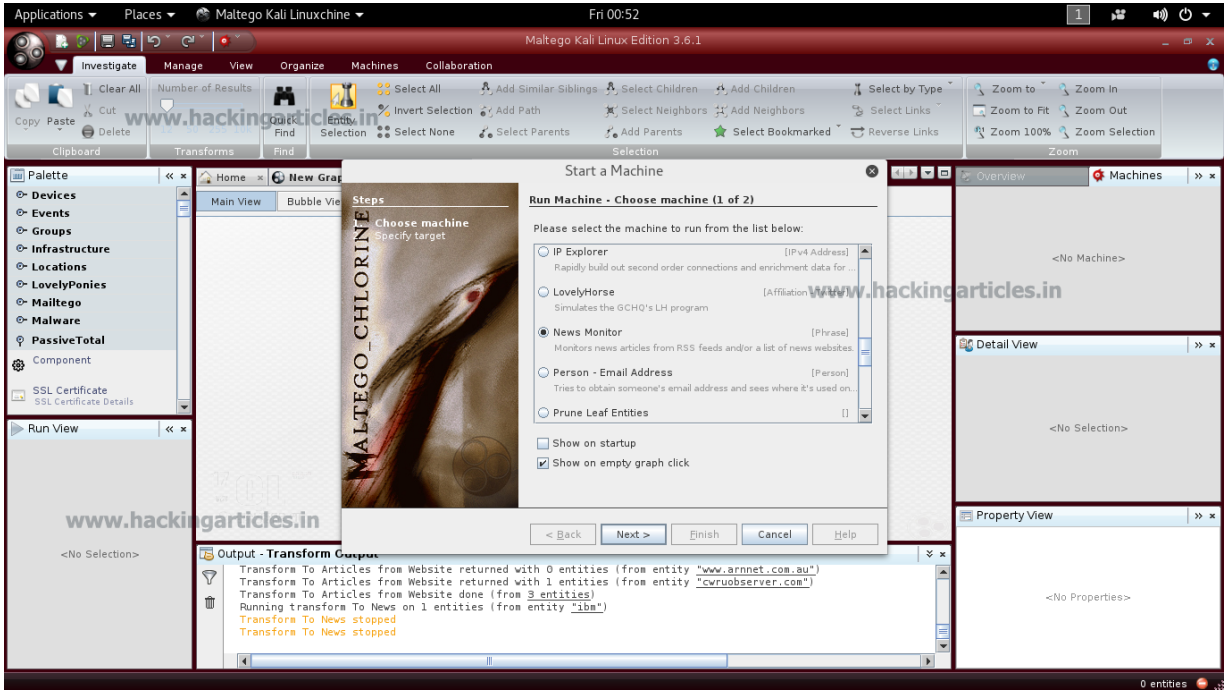


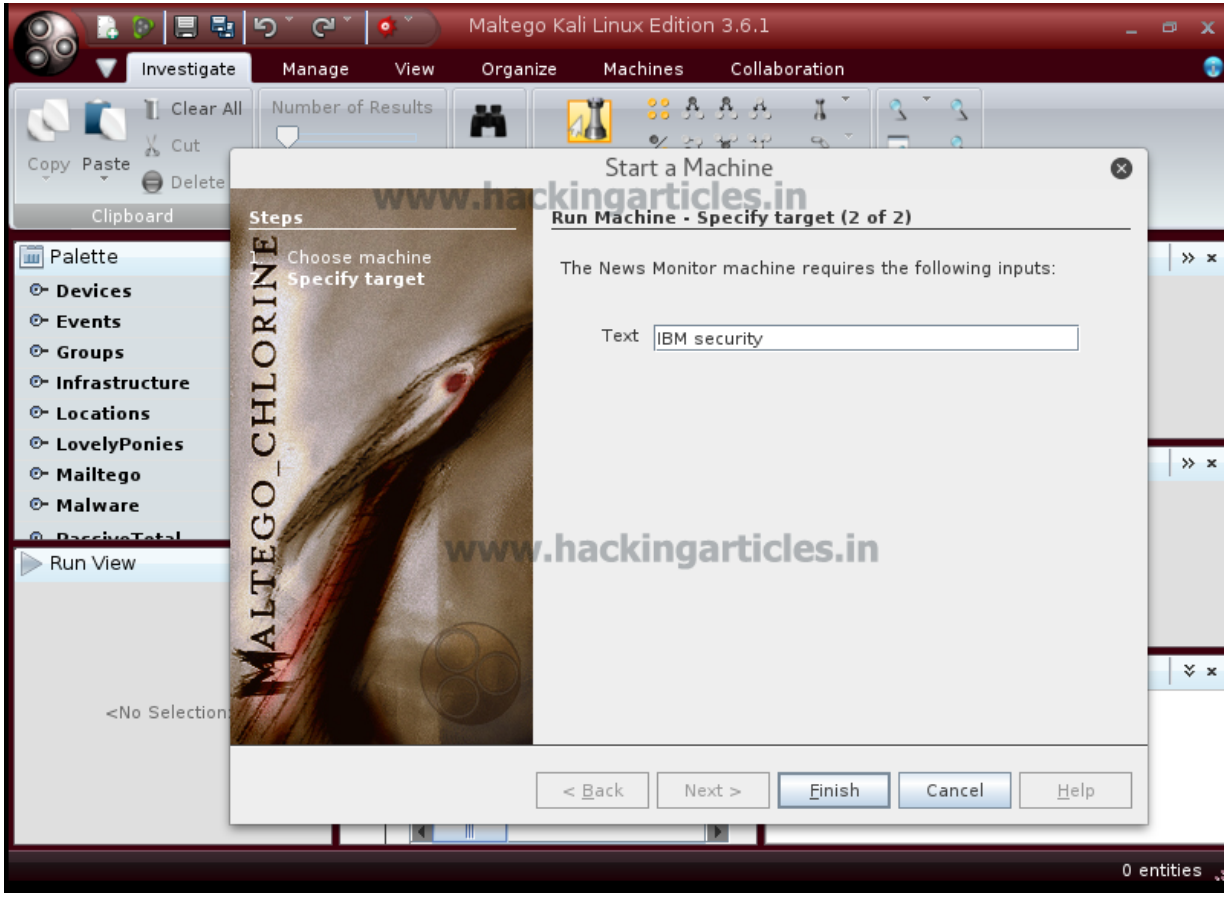
Now enlarge it to clearly view collected data. Here you can see ever information you need like DNS info, mail-server, IP, users, email-ID, connected computers, networks, etc.



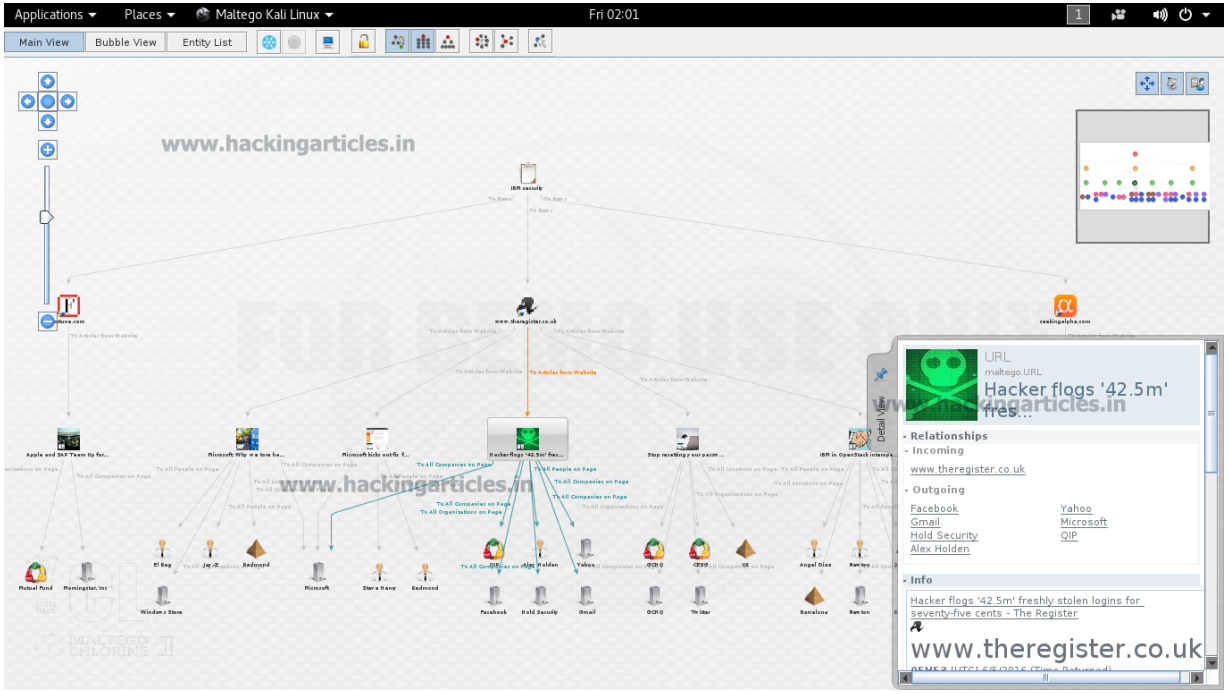
Now let's dig more about this domain, let's see what media or news publishers talking about this company.

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