Practical No 1

DNS Enumeration:

DNS name server and mail server enumeration with dnsenum tool

Syntax: dnsenum <domain name>

Ex: dnsenum example.com

DNS sub-domain enumeration with dnsdict6

Syntax: atk6-dnsdict6 –d46 <domain name>

Ex: atk6-dnsdict6 –d46 example.com

DNS VOIP phone enumeration with dnsrecon

Syntax: dnsrecon –t srv –d <domain name>

Ex: dnsrecon –t srv –d example.com

Practical No 2:

Web site technical information gathering using whatweb tool

This tool will give you information about the target ip, web server fingerprint, server location, back-end app engine along with version number, and any other technical information like google analytics id etc.

Syntax: whatweb –v <domain name>

Ex: whatweb –v example.com

Practical No 3:

Web site technical information gathering using OWASP mantra browser

Please go to http://www.getmantra.com and download the suitable version of OWASP mantra for your pc and install it as soon as it completes.

OWASP mantra is a hacker friendly browser which includes all hacking plugins inbuilt in the browser itself so no need to install them separately.

In this browser whatever website you are trying to open OWASP mantra will automatically get the website information for you.

Practical No 4:

Google Dorks:

intitle

Specifying intitle, will tell google to show only those pages that have the term in their html title. For example intitle:"login page" will show those pages which have the term "login page" in the title text.

allintitle

Similar to intitle, but looks for all the specified terms in the title.

inurl

Searches for the specified term in the url. For example inurl:"login.php".

allinurl

Same as inurl, but searches for all terms in the url.

filetype

Searches for specific file types. filetype:pdf will looks for pdf files in websites. Similarly filetype:txt looks for files with extension .txt

ext

Similar to filetype. ext:pdf finds pdf extension files.

intext

Searches the content of the page. Somewhat like a plain google search. For example intext:"index of /".

allintext

Similar to intext, but searches for all terms to be present in the text.

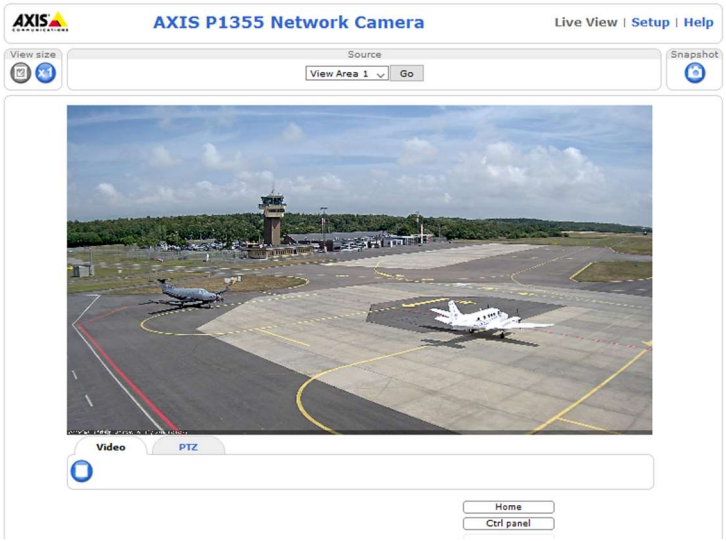
site

Limits the search to a specific site only. site:nullbyte.com

So you can mix them up to find out cameras like this

Inurl:/view/index.shtml

One of the link was opened below and you can see an airport view with planes in it.



We will get even more, but I thought for example one is enough.

If you want more camera google dorks you can follow the below link

http://members.upc.nl/a.horlings/doc-google.html

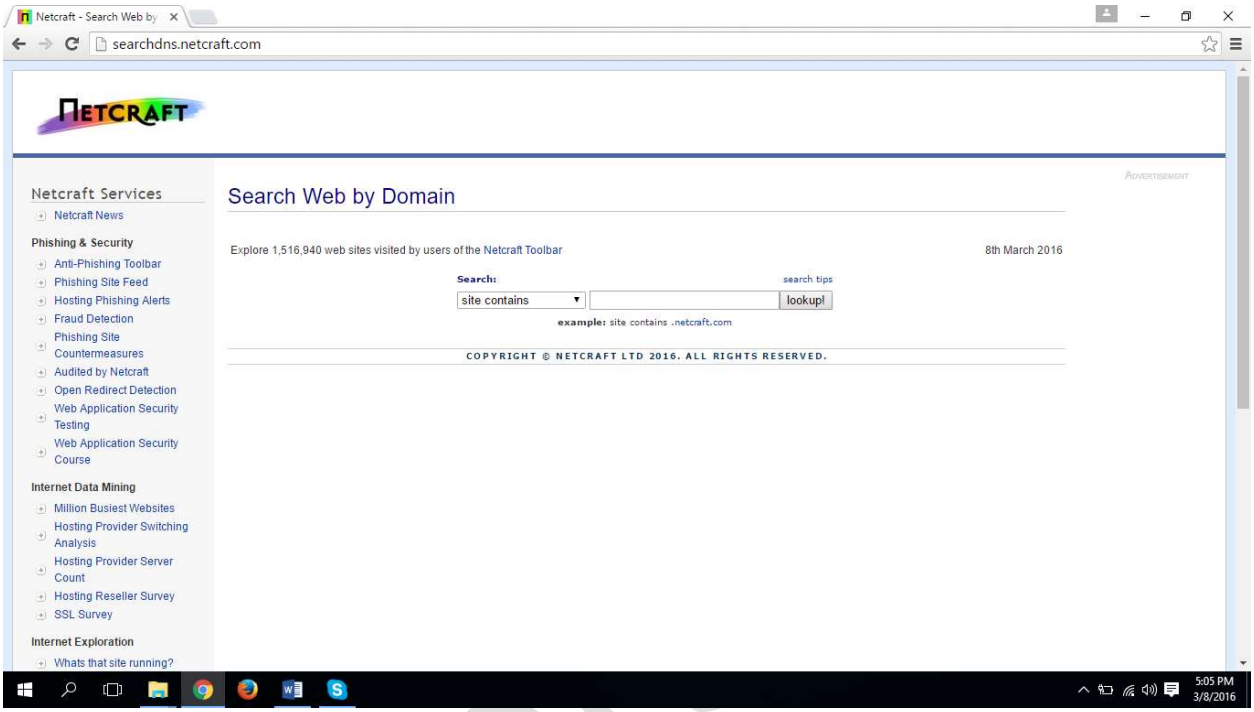
If you want to find out google dorks other than cameras you can follow this link http://www.exploit-db.com

There you can find out google dorks for different categories like files containing usernames, files containing passwords like that.

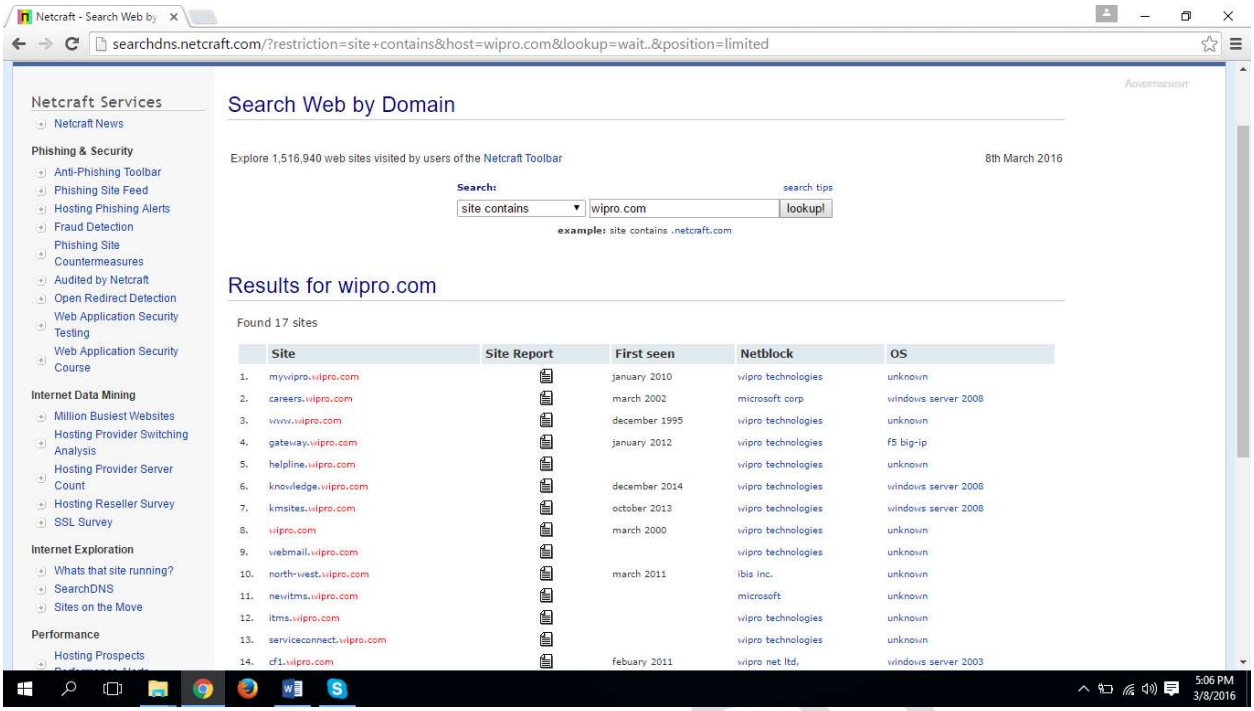
Practical No: 5

You can visit the website searchdns.netcraft.com for gathering information like the hosting history, and site technologies, OS they run on their webservers and the webserver versions etc.

Step 1: open searchdns.netcraft.com website.

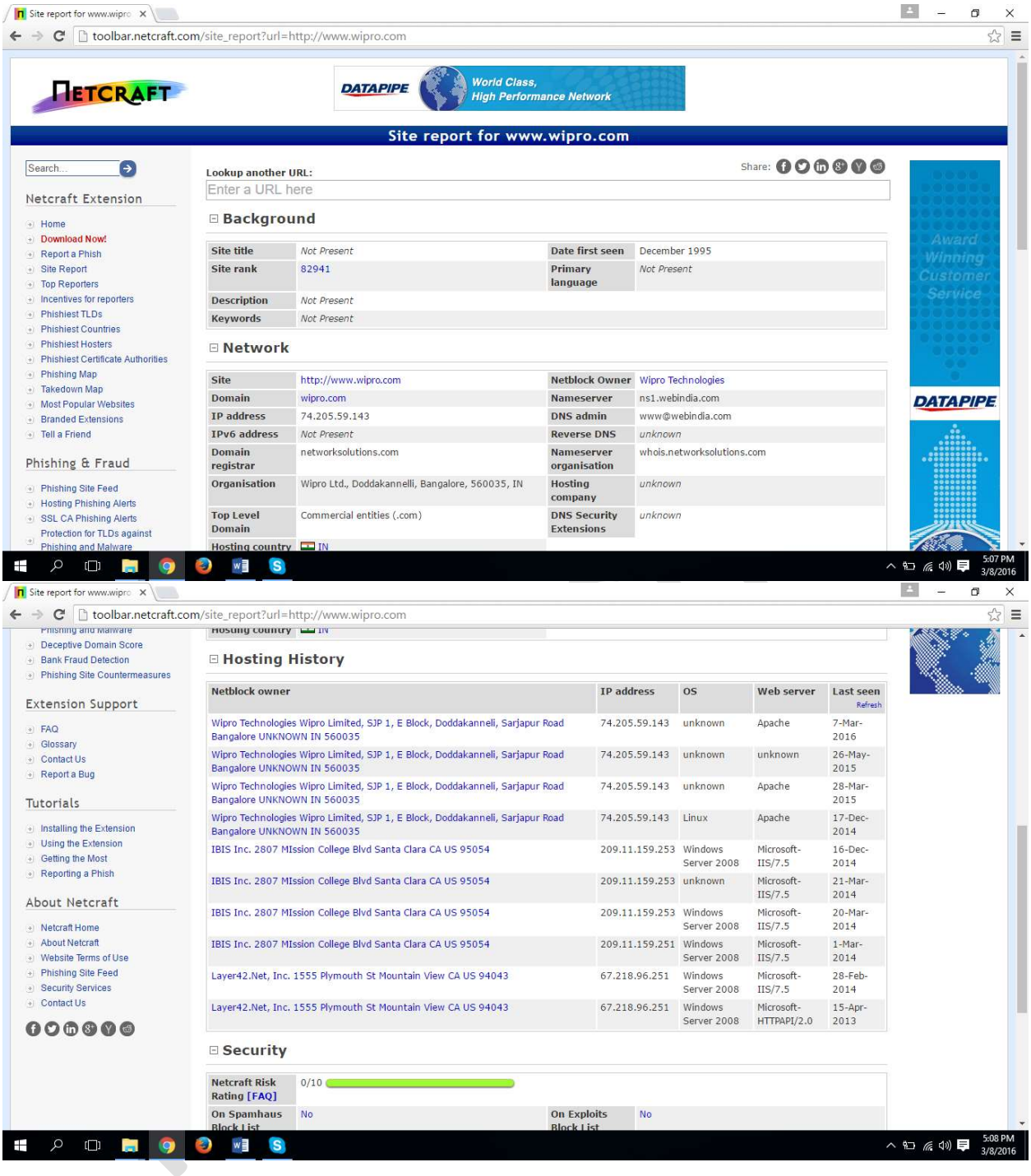


Step 2: enter your domain in search bar and hit lookup button. So you will get result like shown in the below image.



You can get instant results like OS, netblock and firstseen details of the respective domain names.

If youwant more details apart from them click on the site report page icon to get them. Shown in the below image.


Site report for www.wipro
toolbar.netcraft.com/site_report?url=http://www.wipro.com
NETCRAFT
DATAPIPE
World Class, High Performance Network
Site report for www.wipro.com
Search...
Lookup another URL:
Enter a URL here
Share:
Netcraft Extension
Home
Download Now!
Report a Phish
Site Report
Top Reporters
Incentives for reporters
Phishiest TLDs
Phishiest Countries
Phishiest Hosters
Phishiest Certificate Authorities
Phishing Map
Takedown Map
Most Popular Websites
Branded Extensions
Tell a Friend
Phishing & Fraud
Phishing Site Feed
Hosting Phishing Alerts
SSL CA Phishing Alerts
Protection for TLDs against Phishing and Malware
Deceptive Domain Score
Bank Fraud Detection
Phishing Site Countermeasures
Extension Support
FAQ
Glossary
Contact Us
Report a Bug
Tutorials
Installing the Extension
Using the Extension
Getting the Most
Reporting a Phish
About Netcraft
Netcraft Home
About Netcraft
Website Terms of Use
Phishing Site Feed
Security Services
Contact Us
Background
Site title Not Present
Date first seen December 1995
Site rank 82941
Primary language Not Present
Description Not Present
Keywords Not Present
Network
Site http://www.wipro.com
Netblock Owner Wipro Technologies
Domain wipro.com
Nameserver ns1.webindia.com
IP address 74.205.59.143
DNS admin www@webindia.com
IPv6 address Not Present
Reverse DNS unknown
Domain registrar networksolutions.com
Nameserver organisation whois.networksolutions.com
Organisation Wipro Ltd., Doddakannelli, Bangalore, 560035, IN
Hosting company unknown
Top Level Domain Commercial entities (.com)
DNS Security Extensions unknown
Hosting country IN
Award Winning Customer Service
DATAPIPE
5:07 PM 3/8/2016
Hosting History
Netblock owner
IP address
OS
Web server
Last seen
Refresh
Wipro Technologies Wipro Limited, SJP 1, E Block, Doddakanneli, Sarjapur Road Bangalore UNKNOWN IN 560035 74.205.59.143 unknown Apache 7-Mar-2016
Wipro Technologies Wipro Limited, SJP 1, E Block, Doddakanneli, Sarjapur Road Bangalore UNKNOWN IN 560035 74.205.59.143 unknown unknown 26-May-2015
Wipro Technologies Wipro Limited, SJP 1, E Block, Doddakanneli, Sarjapur Road Bangalore UNKNOWN IN 560035 74.205.59.143 unknown Apache 28-Mar-2015
Wipro Technologies Wipro Limited, SJP 1, E Block, Doddakanneli, Sarjapur Road Bangalore UNKNOWN IN 560035 74.205.59.143 Linux Apache 17-Dec-2014
IBIS Inc. 2807 MIssion College Blvd Santa Clara CA US 95054 209.11.159.253 Windows Server 2008 Microsoft-IIS/7.5 16-Dec-2014
IBIS Inc. 2807 MIssion College Blvd Santa Clara CA US 95054 209.11.159.253 unknown Microsoft-IIS/7.5 21-Mar-2014
IBIS Inc. 2807 MIssion College Blvd Santa Clara CA US 95054 209.11.159.253 Windows Server 2008 Microsoft-IIS/7.5 20-Mar-2014
IBIS Inc. 2807 MIssion College Blvd Santa Clara CA US 95054 209.11.159.251 Windows Server 2008 Microsoft-IIS/7.5 1-Mar-2014
Layer42.Net, Inc. 1555 Plymouth St Mountain View CA US 94043 67.218.96.251 Windows Server 2008 Microsoft-IIS/7.5 28-Feb-2014
Layer42.Net, Inc. 1555 Plymouth St Mountain View CA US 94043 67.218.96.251 Windows Server 2008 Microsoft-HTTPAPI/2.0 15-Apr-2013
Security
Netcraft Risk Rating [FAQ] 0/10
On Spamhaus Block List No
On Exploits Block List No
5:08 PM 3/8/2016

Practical No: 6

IP tracking using tracking mail

We can track the victim ip address by sending him an email tracking script to his email for this purpose you can use lot of services, one of them is readnotify.

Follow the below given steps to track an ip address of the victim.

Step 1: open readnotify.com and create an account in that website.

For free account you can send up to 25 ip tracking emails.

Step 2: after logging inside of the website just go towards bottom right corner. There you can find out "member utilities" hover your mouse over that object you can observe a list will appear, select "email quick send" option,

Step 3: on the email quicksend option compose email according to requirement and make sure you add your target email id in the "To" text field along with you target email id append ".readnotify.com" extra like this

target@gmail.com to target@gmail.com.readnotify.com

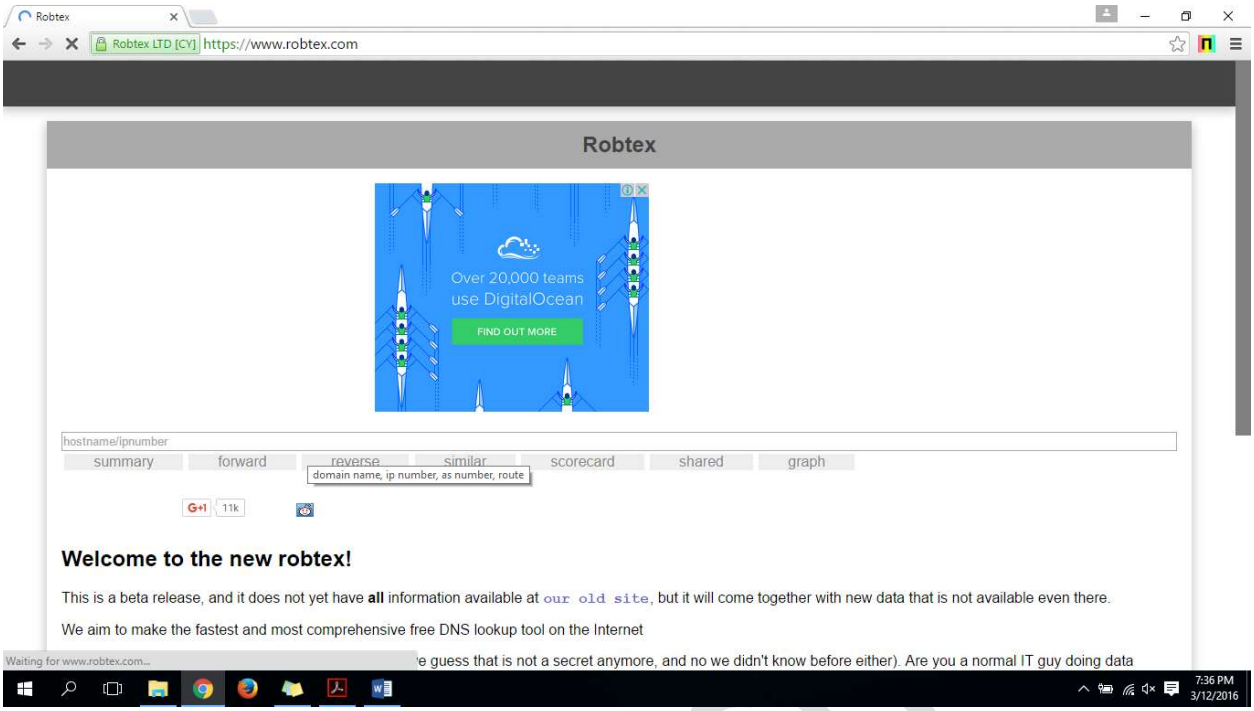
and eventually click on the send button.

Step 4: now again hover your mouse over member utilities and this time select "personal tracking page"

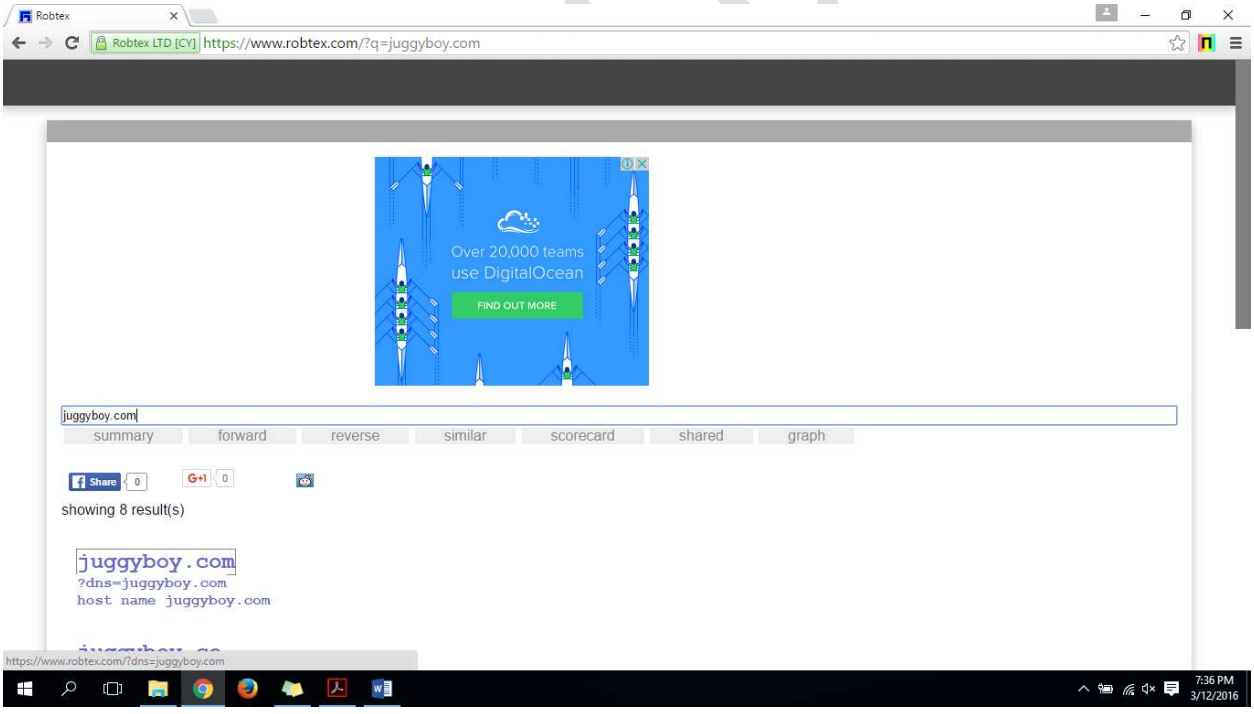
There you can see the list of emails you send to all the victims till now, If he opens your email you can see opened date and time. Click on the date and time to see what ip address the victim is using on that time.

Practical No 7: Using Robtex.com website to get the target website network structure.

Step 1: Go to robtex.com

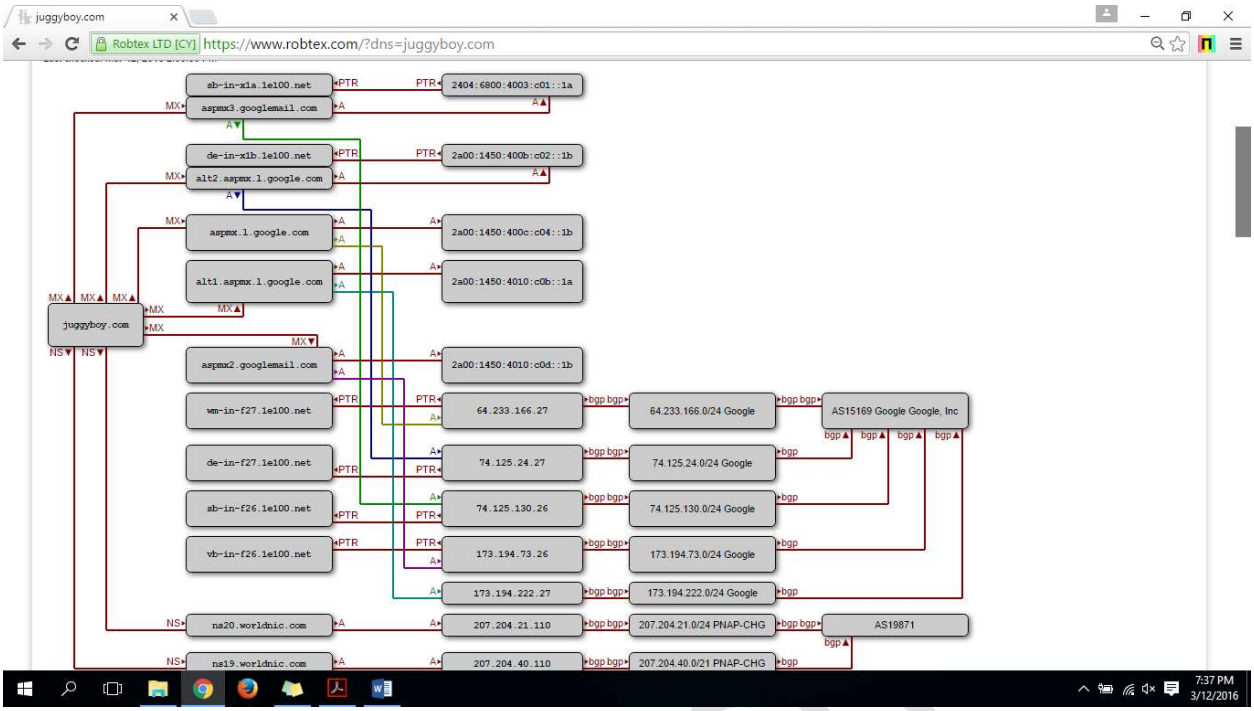


Step 2: Enter your target domain name or IP address into the input box



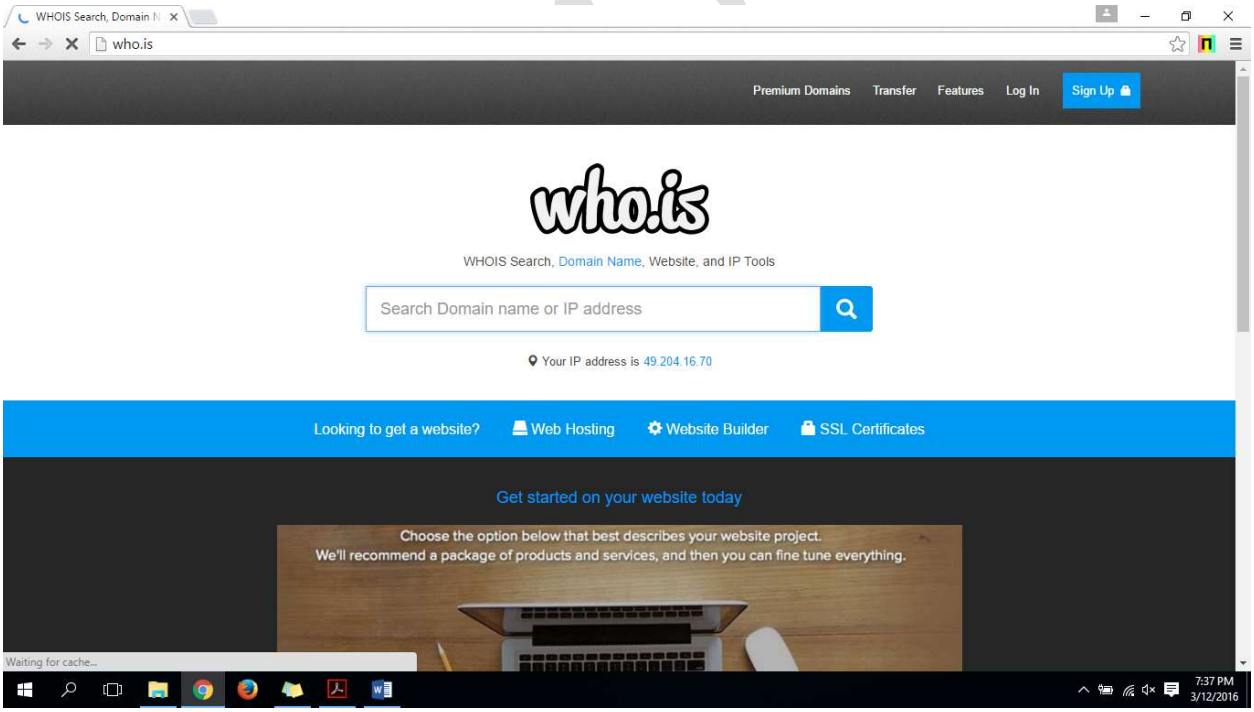
Select the website from the results

Step 3: scroll down to see the network diagram.

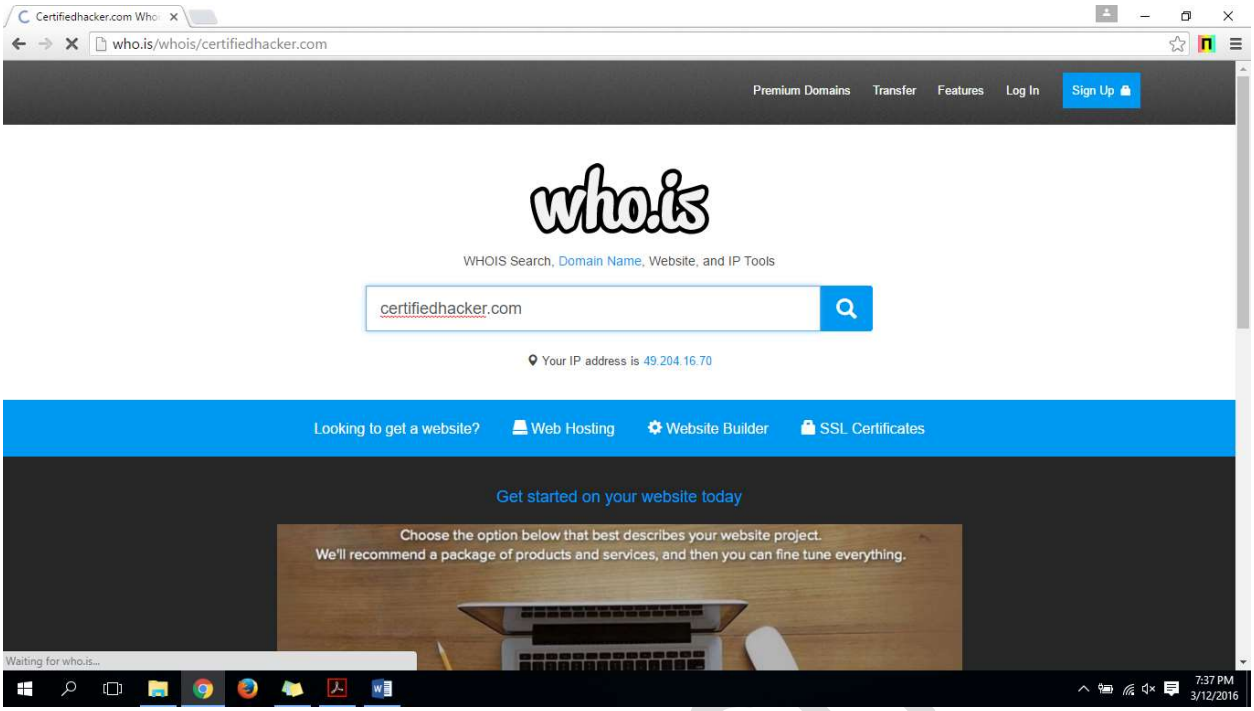


Practical No 8: Using Who.is website to get domain owners information

Step 1: Go to who.is



Step 2: Enter your target domain name or IP address into the input box



Step 3: Get the domain registration information (probably the owner information)