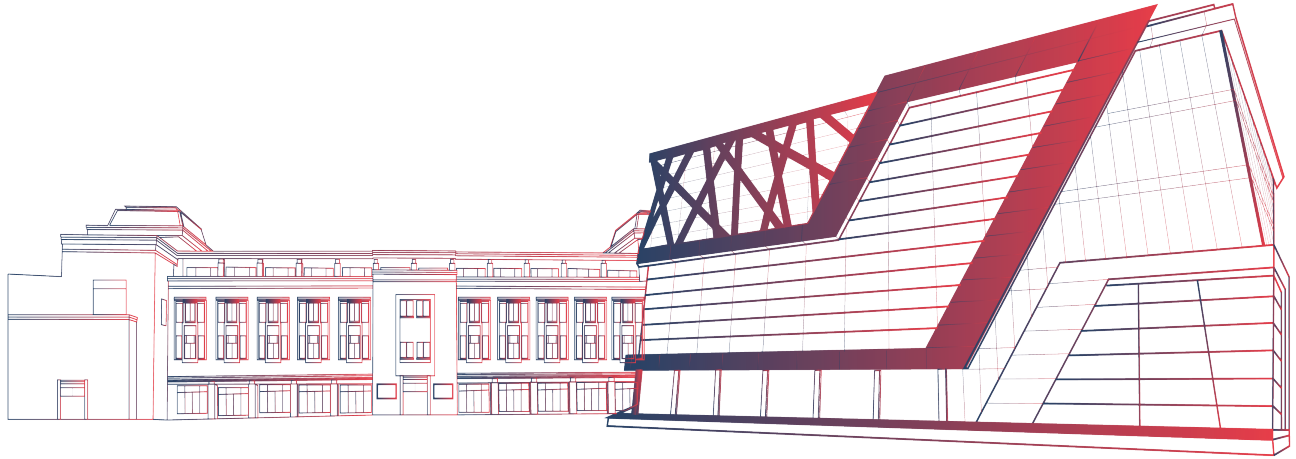
THE NORTHCAP UNIVERSITY

Information Gathering Basics & Tools



30 YEARS OF EXCELLENCE

NAAC Accredited

Reconnaissance or Open Source Intelligence (OSINT) gathering

- OSINT gathering is an important first step in penetration testing.
- Gathering as much intelligence on your organization and the potential targets for exploit.
- Clear understanding of the client's systems and operations before you begin exploiting.
- (how a target works and its potential vulnerabilities.)

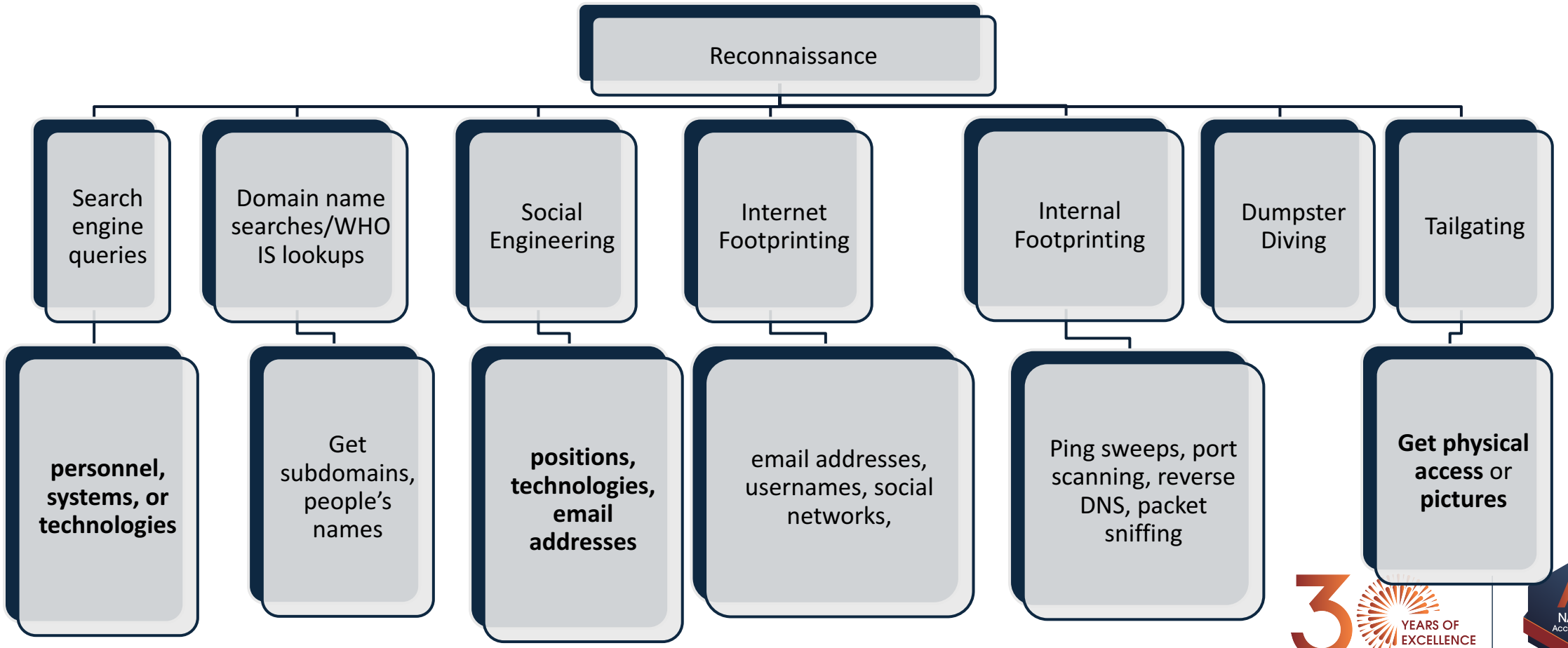
Information Gathering

E.g. Gathering is like breaking into a house.

There’s no need to break down the door to get inside when there **is a window open**.

if the company we are testing has **left any doors unlocked** or maybe a **window open.**

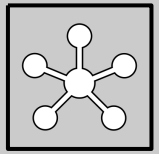
Common reconnaissance include



TYPES OF INFORMATION GATHERING

THE NORTHCAP UNIVERSITY

1. WEB BASED INFORMATION



2. NETWORK BASED INFORMATION GATHERING

3. INDIVIDUAL INFORMATION GATHERING

EXCELLENCE

NAAC Accredited

1. WEB BASED INFORMATION GATHERING :

identify the **services, website and its owner related details.**

services of the Website it is using,

what are the **directories a Web Application** is having,

Server type whether it is using a **Shared Server or a Dedicated Server** etc.

Some Useful Tools -

- https://whois.icann.org/en ,
- https://whois.domaintools.com/,
- https://mxtoolbox.com/

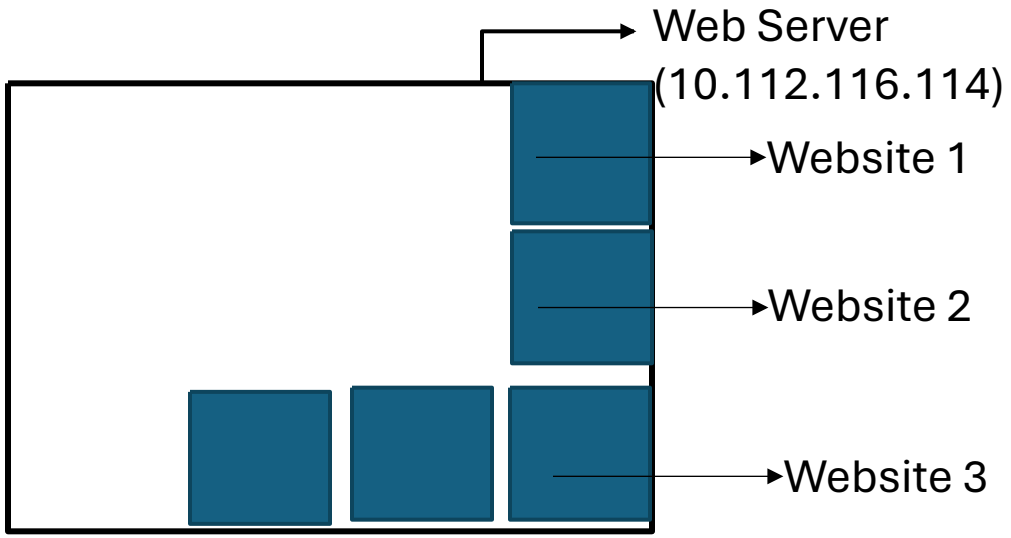
To understand

If some says website is hacked, website is not hacked.

Webserver is hacked.

Website is a **folder called web directories**

If you access of one folder (website) technically you have **entered into the server.**



Webservers

- 2 types of Web Servers
- Shared Webservers
- Dedicated Webservers

Shared Web servers

THE NORTHCAP UNIVERSITY

Many websites with multiple owners on same servers

- Allows multiple websites to utilize a single **server**.
- the most economical option for hosting,
- Overall cost of **server** maintenance is amortized over many customers.

Disadvantages

- **Higher risk** of attack
- Bad neighbours on a shared server **can get the entire IP address blacklisted**
- Unexpected bursts of **web traffic** could **drain the server's limited bandwidth resources.**
- This leads to **slow response time** and **slow loading time**

NAAC Accredited

Dedicated Web servers

THE NORTHCAP UNIVERSITY

Website is the only site hosted on the server.

own dedicated server is the ultimate “fence”.

Extremely **unlikely to get blacklisted**

- Unless organization engages in unethical or illegal internet practices.

Website is the only user, there are fewer chances to acquire

viruses,

malware and

spyware

Because of poor neighbours and misconfigured security.

Disadvantage

High cost
30000-35000

NAAC Accredited

Reconnaissance Tools

- dnsstuff.com- https://www.dnsstuff.com/
- Netcraft.com- https://toolbar.netcraft.com/site_report
- Yougetsignal.com- https://www.yougetsignal.com/
- Whois.icann.org - https://lookup.icann.org/, ttps://whois.icann.org/en/about-whois
- whois.domaintools.com- https://whois.domaintools.com
- Mxtoolbox.com- https://Mxtoolbox.com
- Ip2location.com- https://Ip2location.com
- Ip-tracker.com- https://Ip-tracker.com
- Wappalyzer.com- add as extension/ plugin
- etc

Tool 1

Dnsstuff.com

THE NORTHCAP UNIVERSITY

It has lot of tools which provide information https://tools.dnsstuff.com/

Domain tools

- Whois lookup
- DNS lookup
- SSL examination- domain is using SSL or not
- Generates report

IP tools

- Reverse DNS-country tool – IP ranges for country
- DNS Root Server Response Time

Networking tools

- DNS Traversal
- DNS Timing

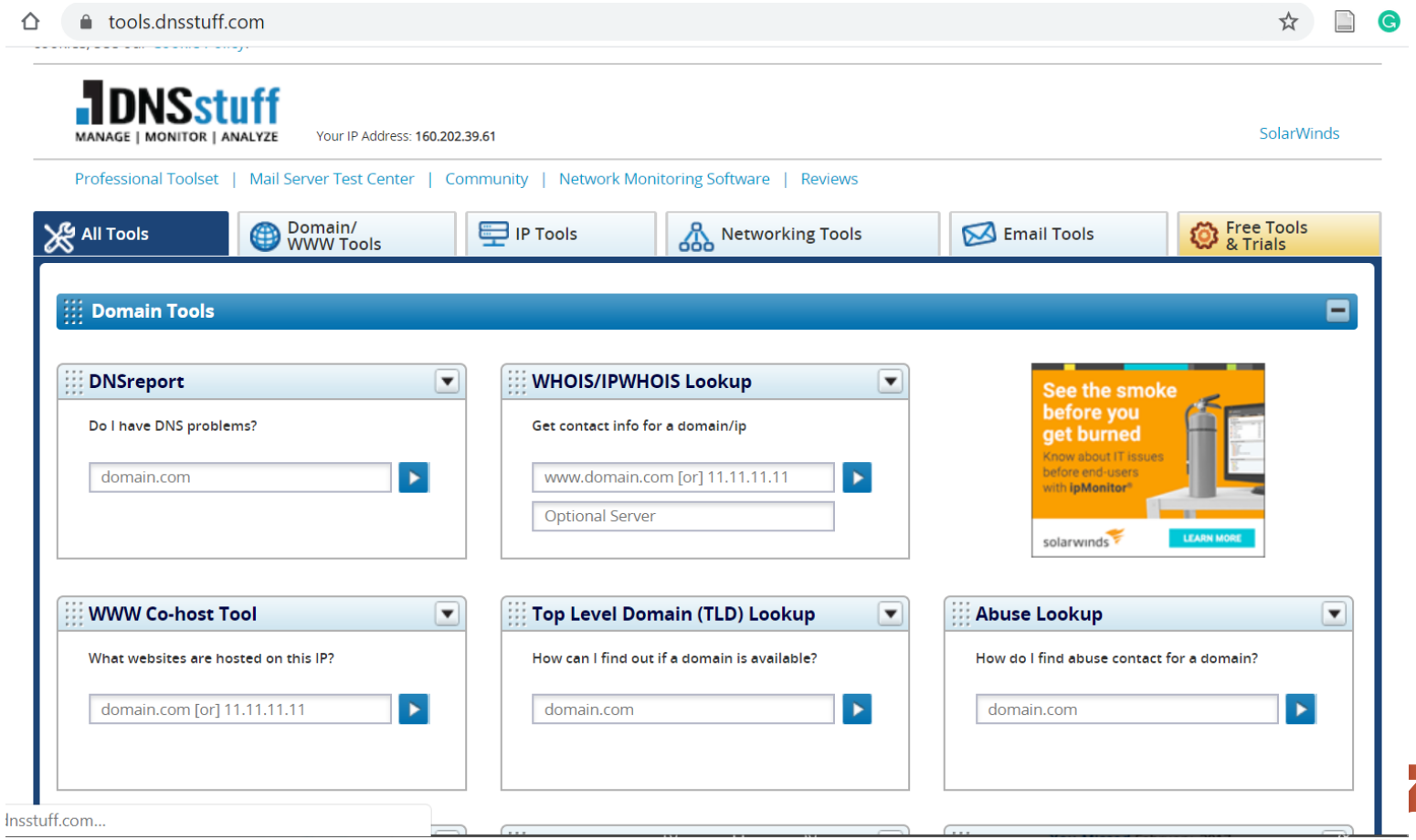
Email tools

- Email Test
- Spam blacklist lookup
- Email path analyser

EXCELLENCE

NAAC Accredited

Dnsstuff.com



Dnsstuff.com- DNSReport

THE NORTHCAP UNIVERSITY

DNSreport

- It generates report
- It gives details of parent zone DNS servers
- Records open DNS server
- Generate Report & analyse- 5 mins Task

EXCELLENCE

NAAC Accredited

Dnsstuff.com- DNSReport

THE NORTHCAP UNIVERSITY

DNSreport Results for ncuindia.edu — Export

Overall Results: 0 FAIL | 4 WARNING | 27 PASS | 5 INFO

PARENT

Status	Test Name	Information
WARN	Parent zone provides NS records	Parent zone does not provide glue for nameservers, which will cause delays in resolving your domain name. The following nameserver addresses were not provided by the parent 'glue' and had to be looked up individually. This is perfectly acceptable behavior per the RFCs. This will usually occur if your DNS servers are not in the same TLD as your domain (for example, a DNS server of "ns1.example.org" for the domain "example.com"). In this case, you can speed up the connections slightly by having NS records that are in the same TLD as your domain. ns-249.awsdns-31.com. | No Glue | TTL=172800 ns-721.awsdns-26.net. | No Glue | TTL=172800 ns-1615.awsdns-09.co.uk. | No Glue | TTL=172800 ns-1200.awsdns-22.org. | No Glue | TTL=172800
PASS	Number of nameservers	At least 2 (RFC2182 section 5 recommends at least 3), but fewer than 8 NS records exist (RFC1912 section 2.8 recommends that you have no more than 7). This meets the RFC minimum requirements, but is lower than the upper limits that some domain registrars have on the number of nameservers. A larger number of nameservers reduce the load on each and, since they should be located in different locations, prevent a single point of failure. The NS Records provided are: ns-249.awsdns-31.com. | No Glue | TTL=172800 ns-721.awsdns-26.net. | No Glue | TTL=172800 ns-1615.awsdns-09.co.uk. | No Glue | TTL=172800 ns-1200.awsdns-22.org. | No Glue | TTL=172800

NS

EXCELLENCE

NAAC Accredited

Dnsstuff.com-Whois Lookup

THE NORTHCAP UNIVERSITY

Whois Lookup

- Generate information regarding domain
- Date of domain created
- Domain Updation date
- Source of the information is collected
- Contact details (No privacy- open source)- this is valuable information
- Server information
- Etc.

EXCELLENCE

NAAC Accredited

Dnsstuff.com-Whois Lookup

Ca

WHOIS/IPWHOIS Lookup Results for ncuindia.edu

Results for Target: ncuindia.edu

Created Date :	26-May-2015
Updated Date :	10-Jul-2019
Expires Date :	31-Jul-2022
WHOIS Server:	whois.educause.net

Discovered Nameservers

NS-1200.AWSDNS-22.ORG | 205.251.196.176
NS-1615.AWSDNS-09.CO.UK | 205.251.198.79
NS-721.AWSDNS-26.NET | 205.251.194.209
NS-249.AWSDNS-31.COM | 205.251.192.249

Registrar Information

[NOT DETECTED]

*Please note these results are obtained from third party databases (whois.educause.net)

Contact Information

Registrant

The National Capital University
HUDA Sector 23-A
Gurgaon, 122 017

Administrative Contact

Vijay Daulet-Singh
The National Capital University
HUDA Sector 23-A

Technical Contact

Deepak Satyarthi
The National Capital University
HUDA Sector 23-A

Tool 2

Netcraft

THE NORTHCAP UNIVERSITY

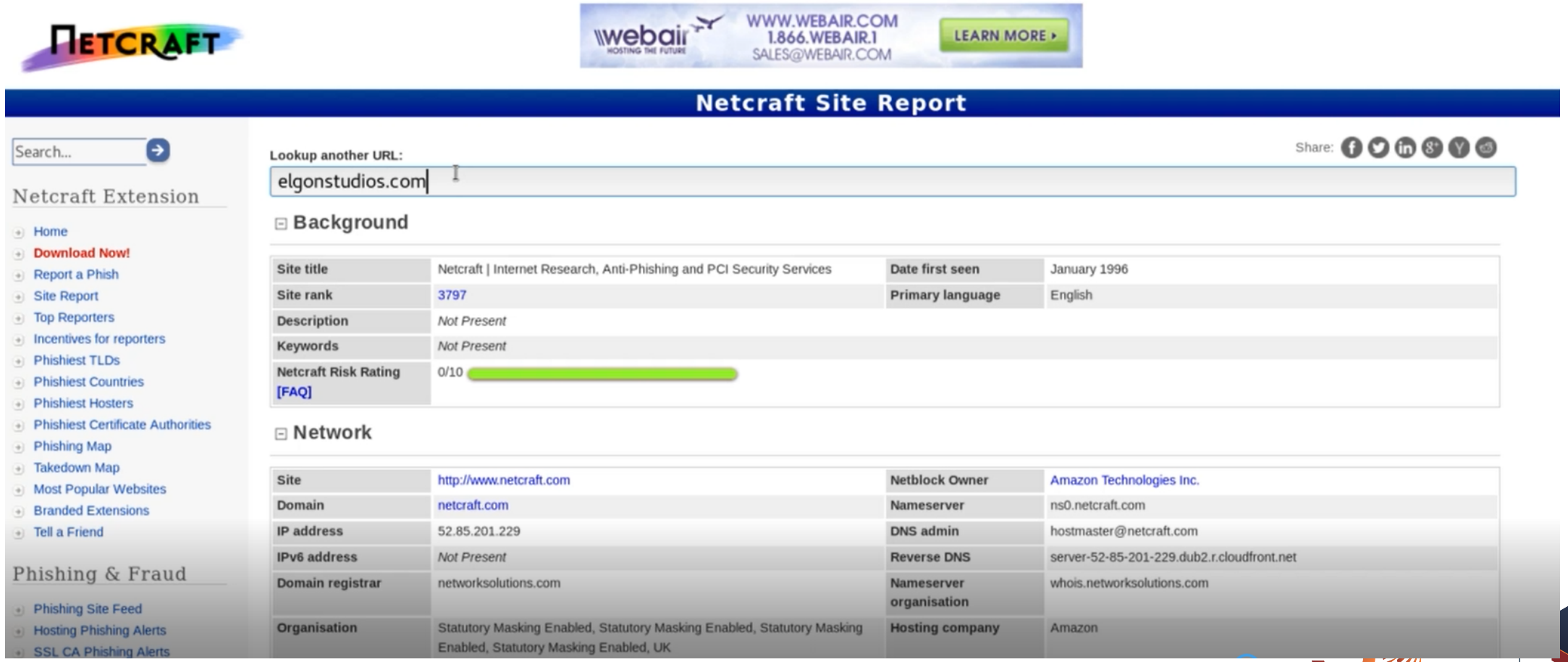
Allows to understand what is running behind the website

- What is IP address on website server it is hosted on
- Web tracker
- Server side technology
- What are the frameworks
- Email
- CMS system
- Domain registrar
- DNS administrator

30 YEARS OF EXCELLENCE

NAAC Accredited

Netcraft: https://www.netcraft.com/



Tool 3

Whois Lookup

THE NORTHCAP UNIVERSITY

You asking database whois to search

Command:

Who is this domain registered to?

More details of the domain etc.

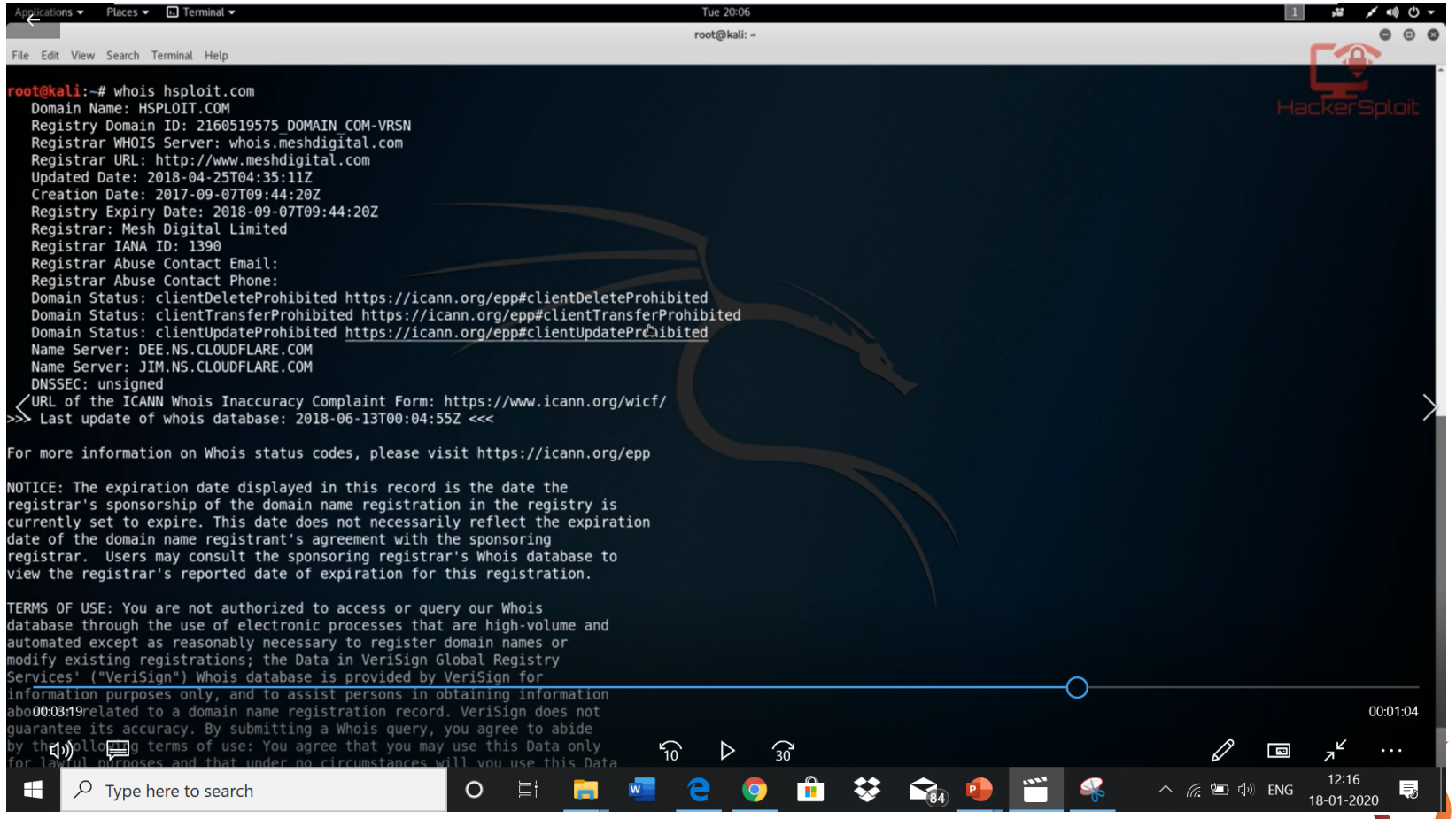
Whois hspolit.com

Can use this tool on Kali Linux

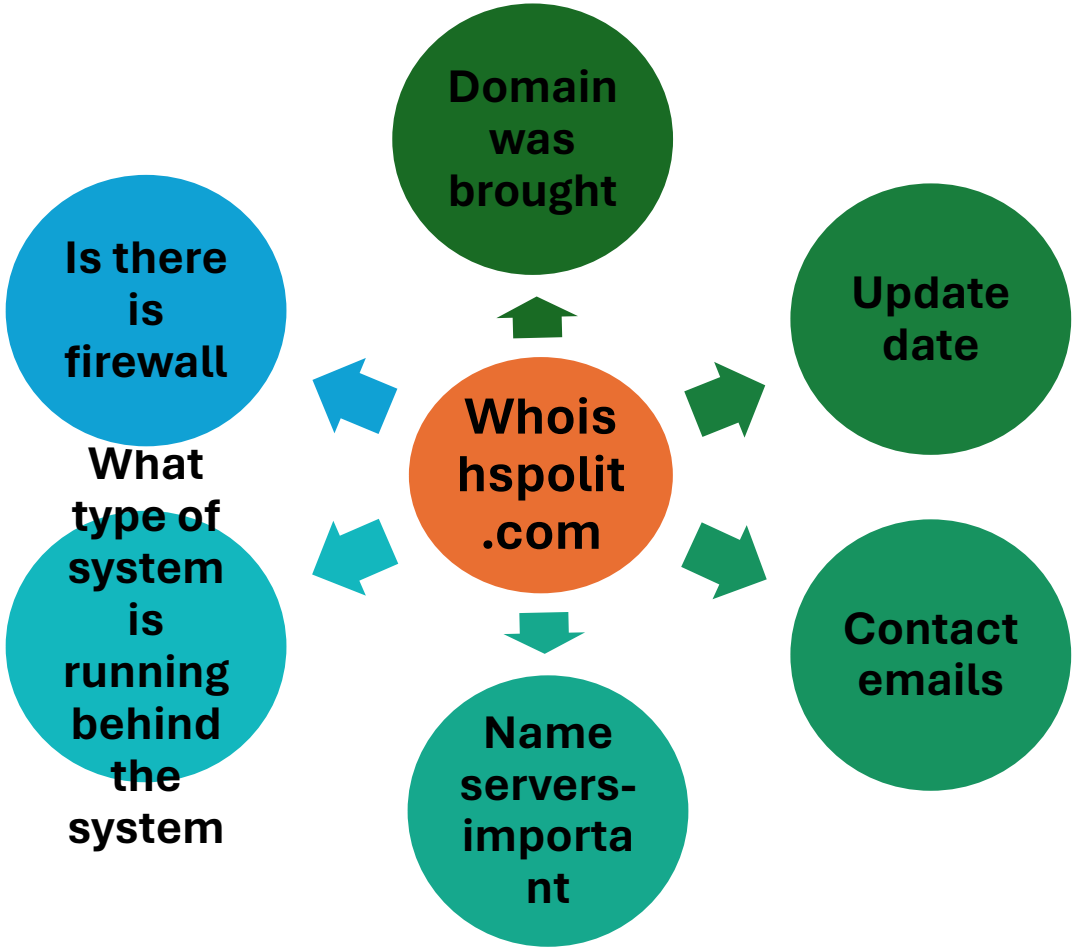
30 YEARS OF EXCELLENCE

NAAC Accredited

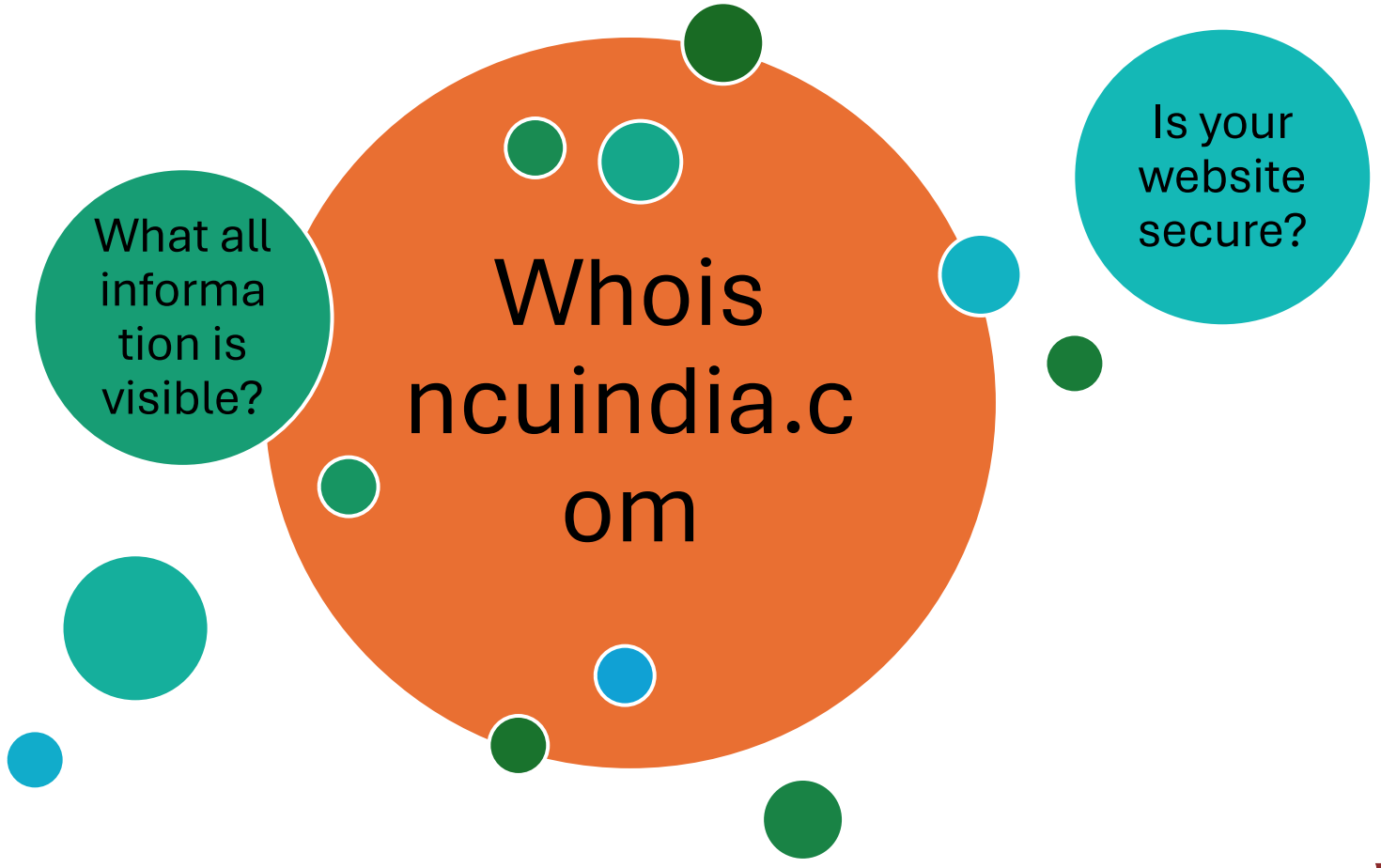
Whois


Applications
Places
Terminal
Tue 20:06
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# whois hsploit.com
Domain Name: HSPLOIT.COM
Registry Domain ID: 2160519575_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.meshdigital.com
Registrar URL: http://www.meshdigital.com
Updated Date: 2018-04-25T04:35:11Z
Creation Date: 2017-09-07T09:44:20Z
Registry Expiry Date: 2018-09-07T09:44:20Z
Registrar: Mesh Digital Limited
Registrar IANA ID: 1390
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: DEE.NS.CLOUDFLARE.COM
Name Server: JIM.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2018-06-13T00:04:55Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
HackerSploit
00:03:19
00:01:04
10
30
Type here to search
ENG
12:16
18-01-2020

Whois Lookup



Whois task- 5 mins (kali Linux)

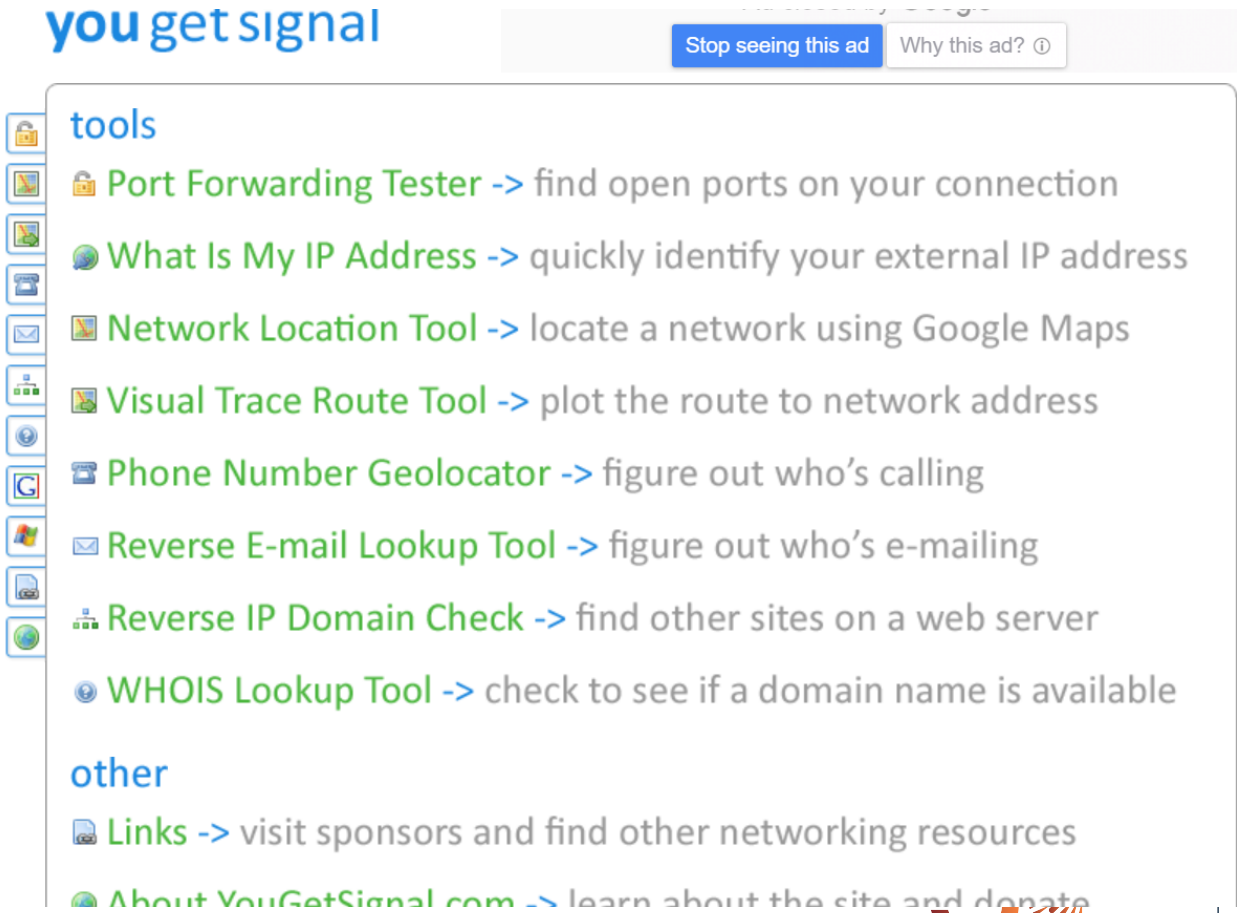


Tool 4

Yougetsignal.com (Tool)

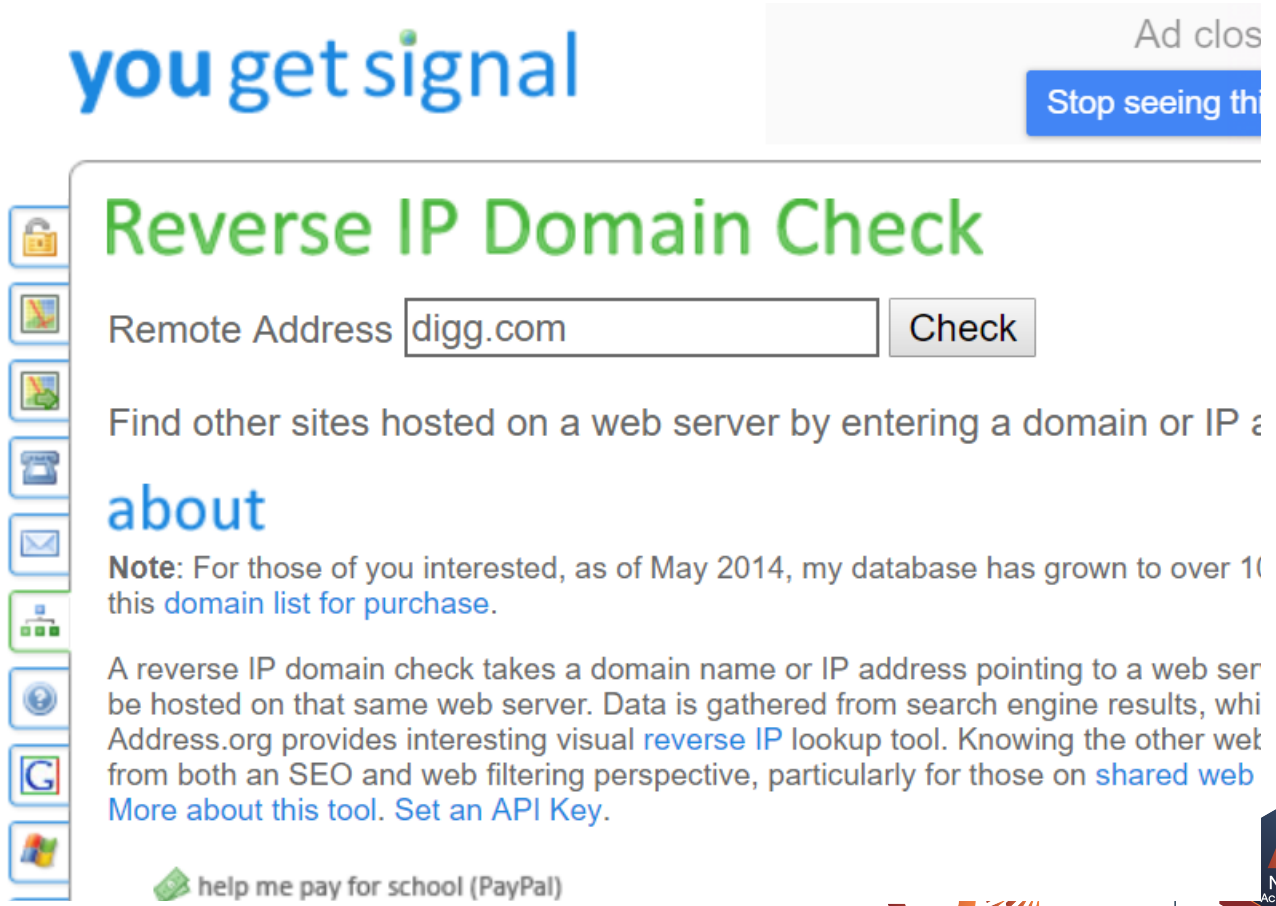
Check many things online

- Shared/Dedicated webserver
- IP address
- Traceroute
- Whois lookup
- Reverse IP domain
- etc



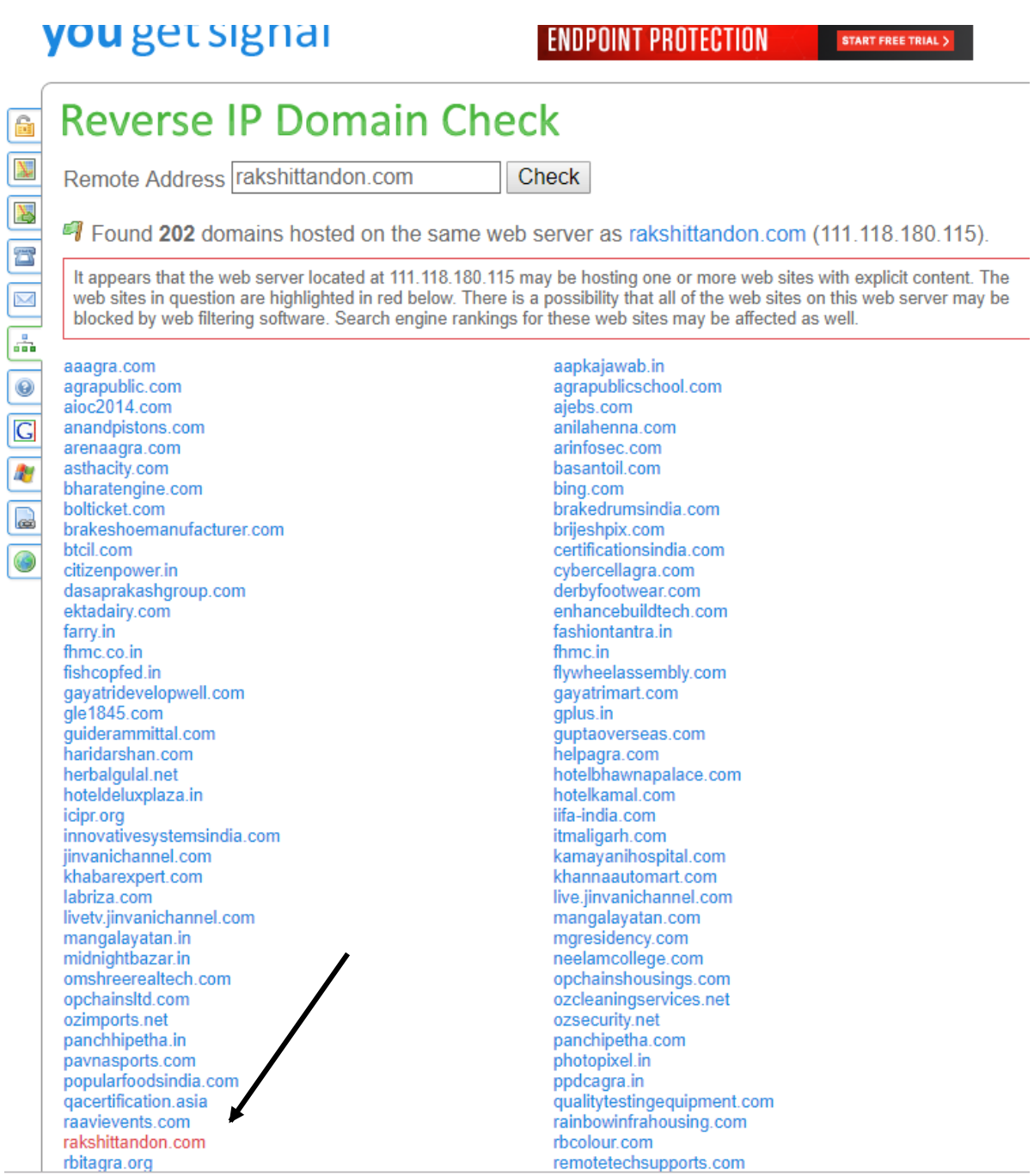
Yougetsignal.com (Tool) ->Reverse IP domain

Check number of domains and
IP address of web server



Yougetsignal.com->Reverse IP domain

- www.google.com, shows all the subdomains of google and shows it uses dedicated web sever.
- www.soch.com it shows 1000 domains hosted on same web server. Therefore it is shared web server
- All websites hosted on same web server have same IP address
- Search www.ncuindia.edu only one domain (dedicated)



THE NORTHCAP UNIVERSITY

Case study

- Rakshit Tandon
- Website was hacked as it was on shared web server where one website was panchipetha.com(hacked).
- Check on yougetsignal.com
- Red colored (reported for spam by someone)

30 YEARS OF EXCELLENCE

NAAC Accredited

Tool 5

whois.icann.org (search on google)

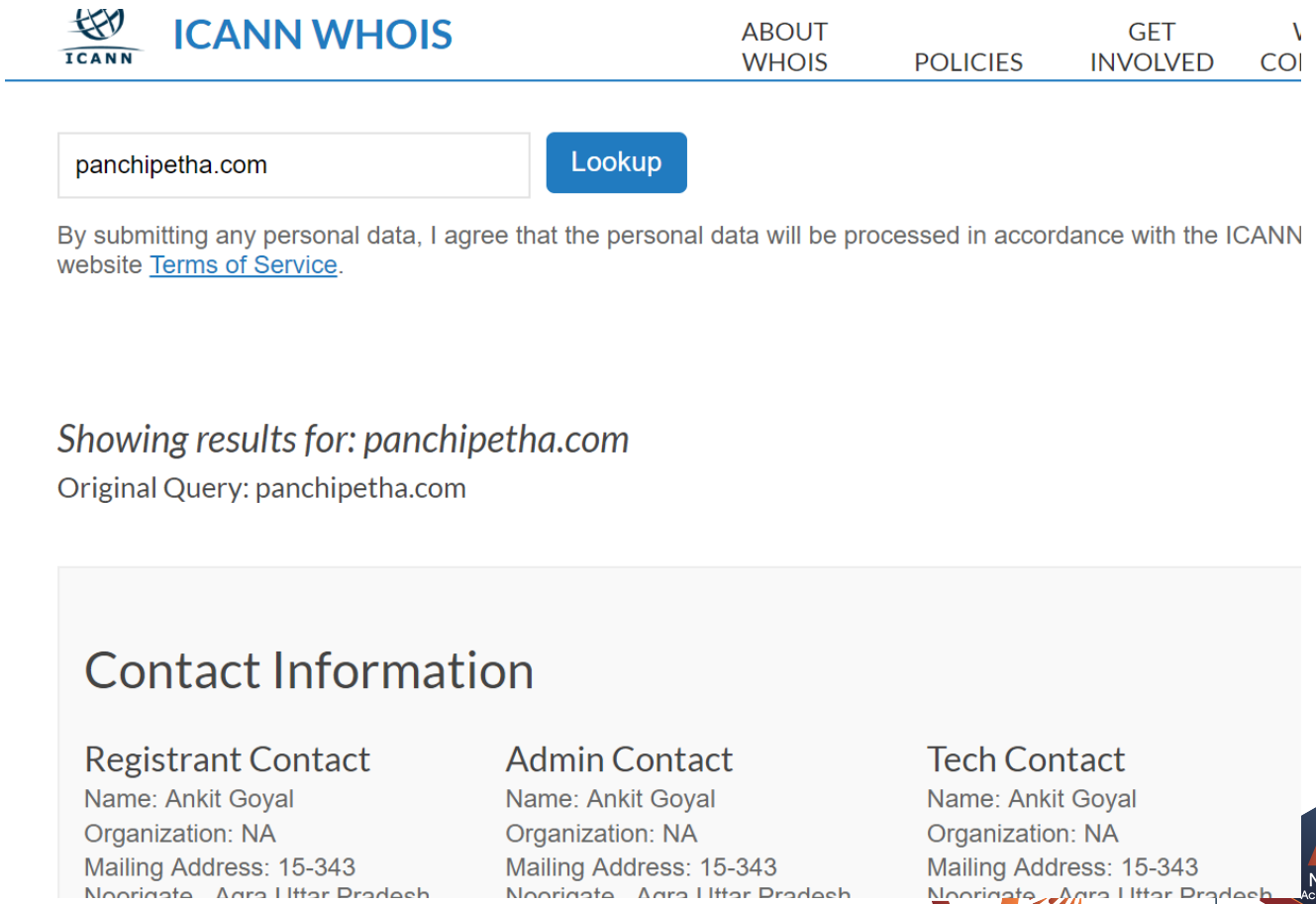
THE NORTHCAP UNIVERSITY

- Whois.icann.org
- ICANN (father) Non-profitable org
- IANA (Son)-paid
- Domain is provided by
- Service Provider (Godaddy.com)

Whois.icann.org

Can see the details of website

- E.g. panchipetha.com



Whois.icann.org

- Can see the details of website
- E.g. Lucideus.com

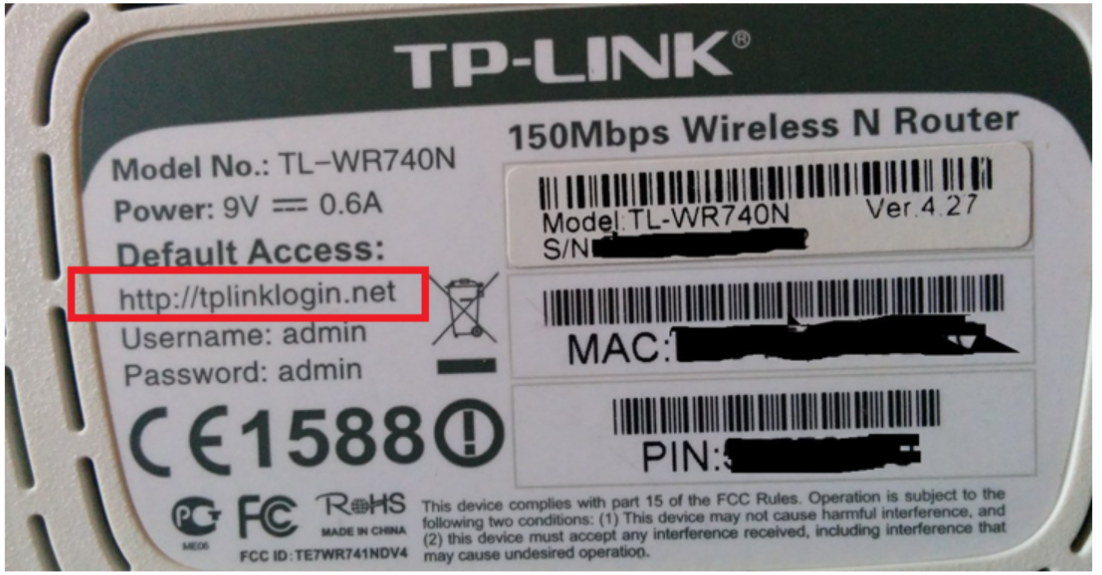
- **No information is revealed**

Case study-search

- TP link forgets to renew the domain, then some other person bought that link... loss to TP link
- TP-Link bought same domain from that person 2.5$million

Oops! TP-Link forgets to Renew and Loses its Domains Use
Configure Router Settings

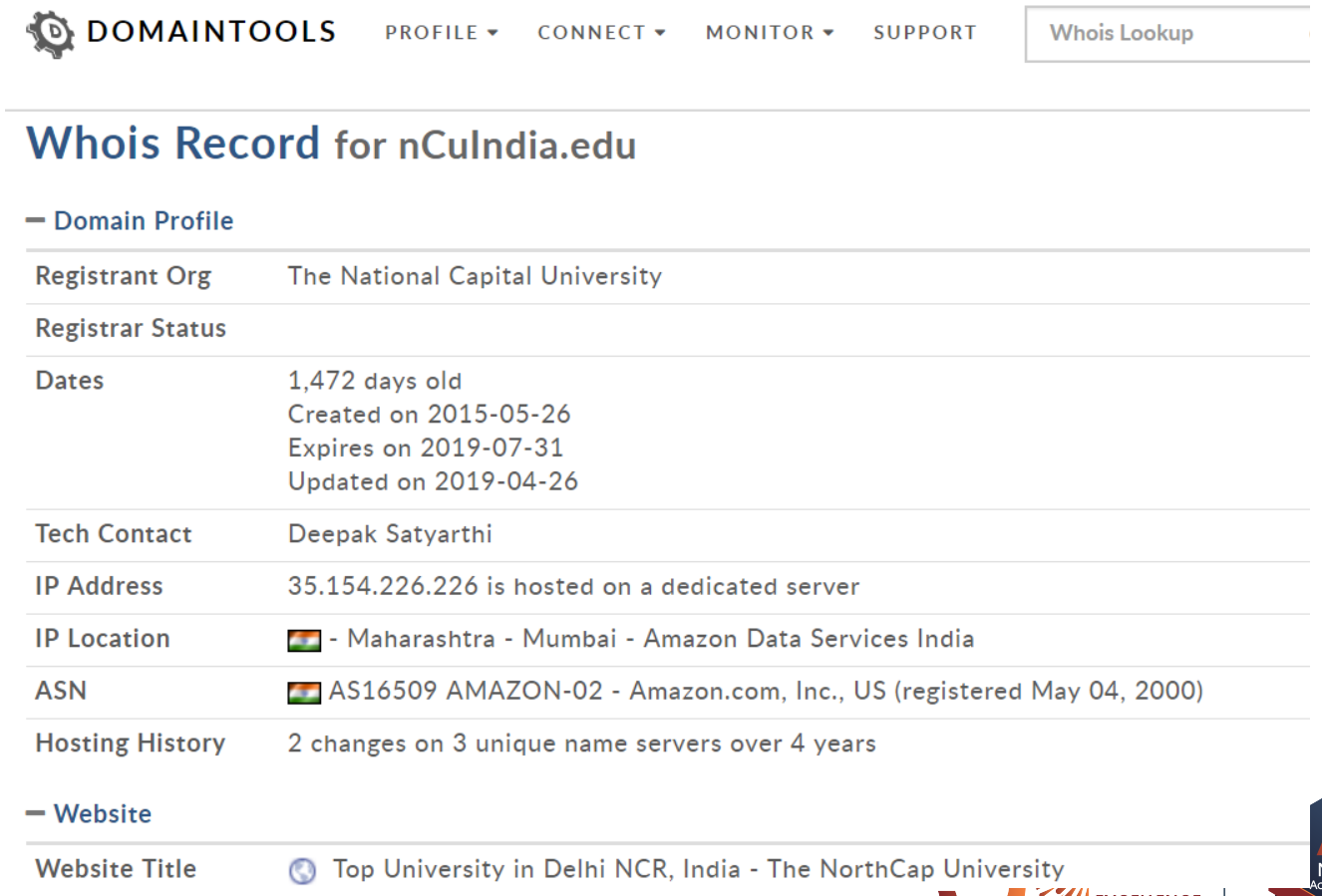
July 06, 2016 Swati Khandelwal



To make the configuration of routers easier, hardware vendors instruct users to browse to a domain name rather than numeric IP addresses.

whois.domaintools.com

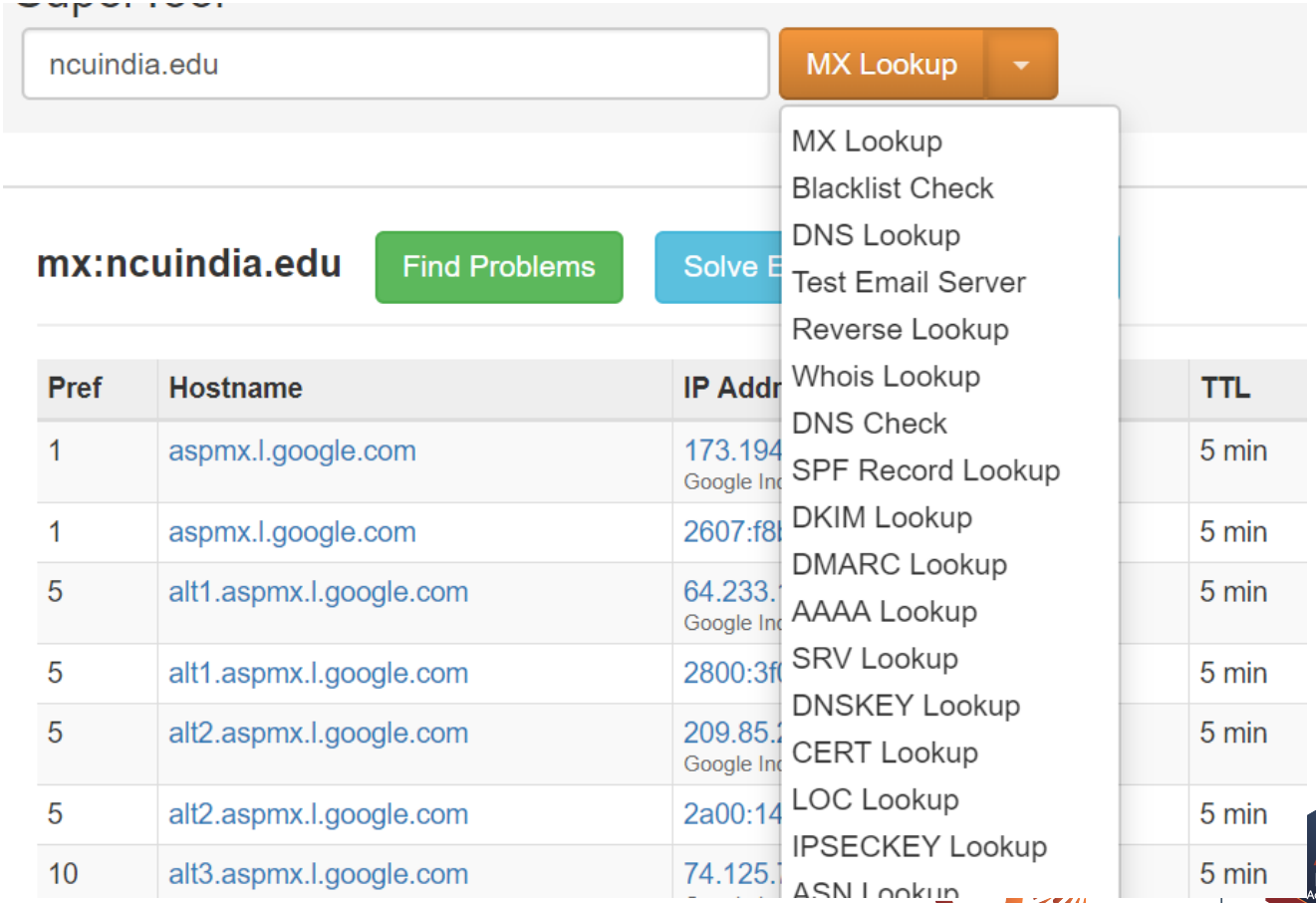
- Network
  - **domains and IPs,**
  - **connects them with nearly every active** domain on the internet.
- IP Location
- Hosting History
- These connections help security **professionals profile attackers, guide online fraud investigations**, and map cyber activity to attacker infrastructure.



Tool 6,7,8,9

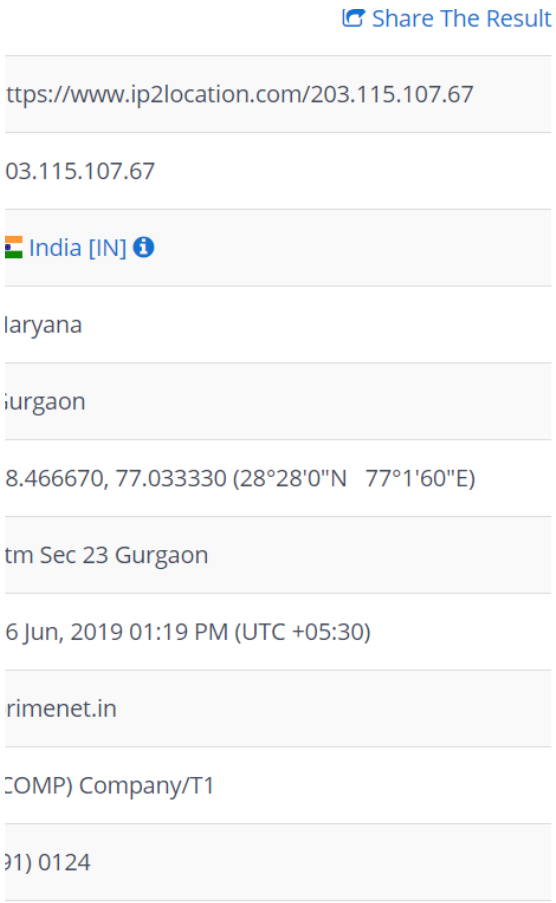
Mxtoolbox.com

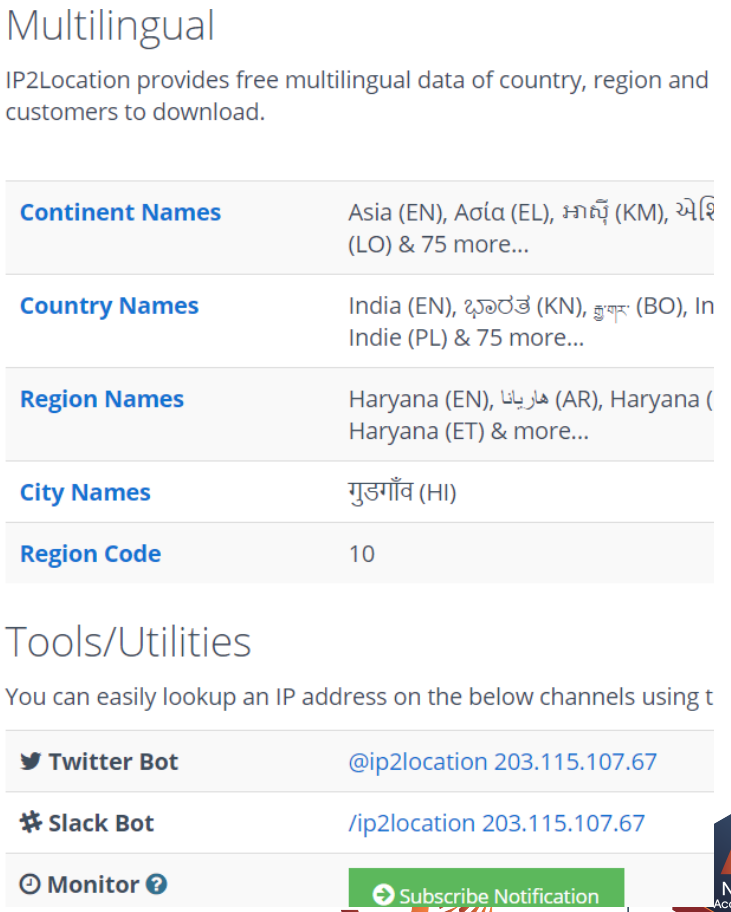
- Lots of information can be revealed through this tool
- It has **drop down menu**
- What ever information is required can be seen from drop down



Ip2location.com

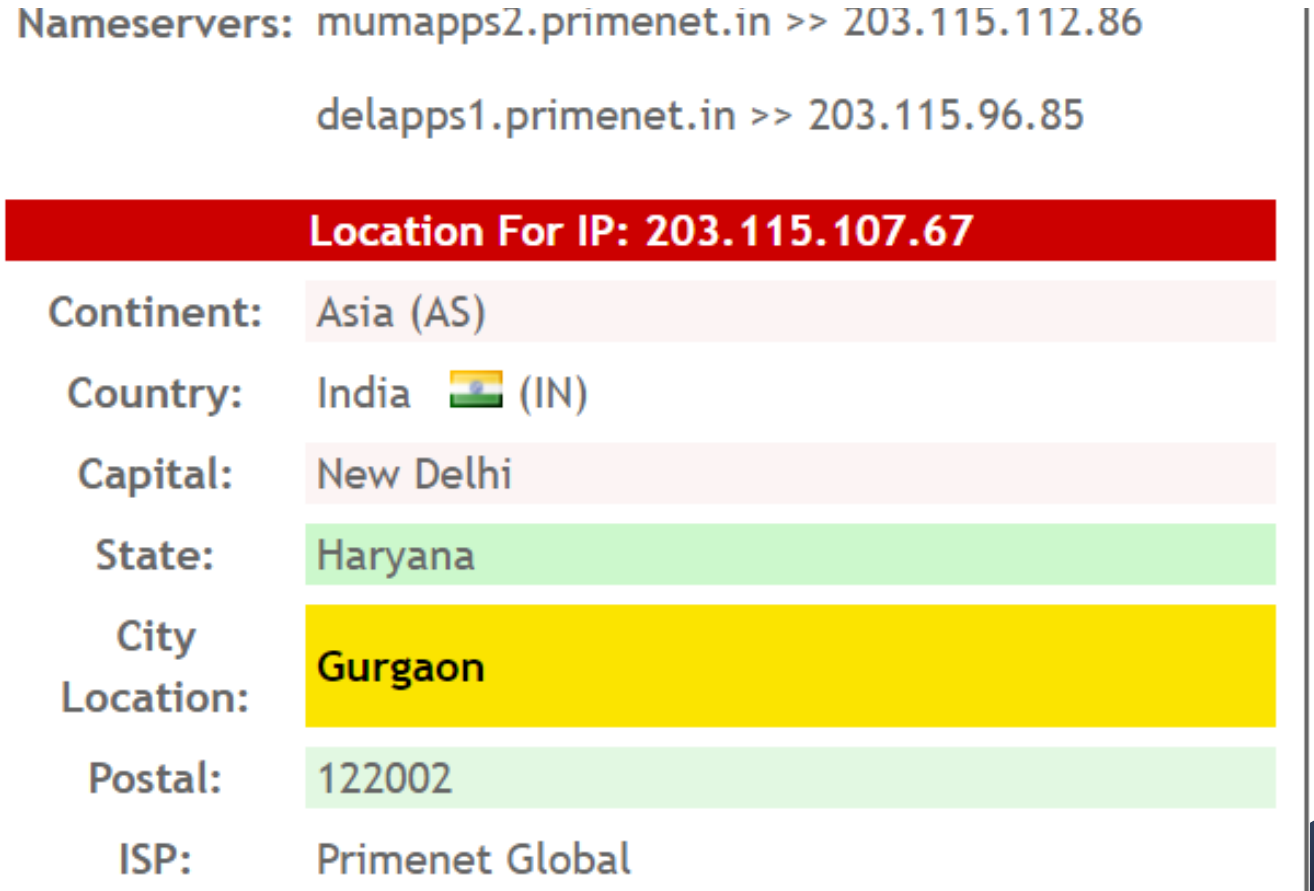
- It takes the IP address and tells the **coordinates of city, domain, city, region, Area code etc**





Ip-tracker.com

- Tool with power and accuracy that **gives you easy way to lookup, find, track and trace any IP** in the world.
- Traces **Internet Protocol Address** and information about **IP location and other related information to your IP**

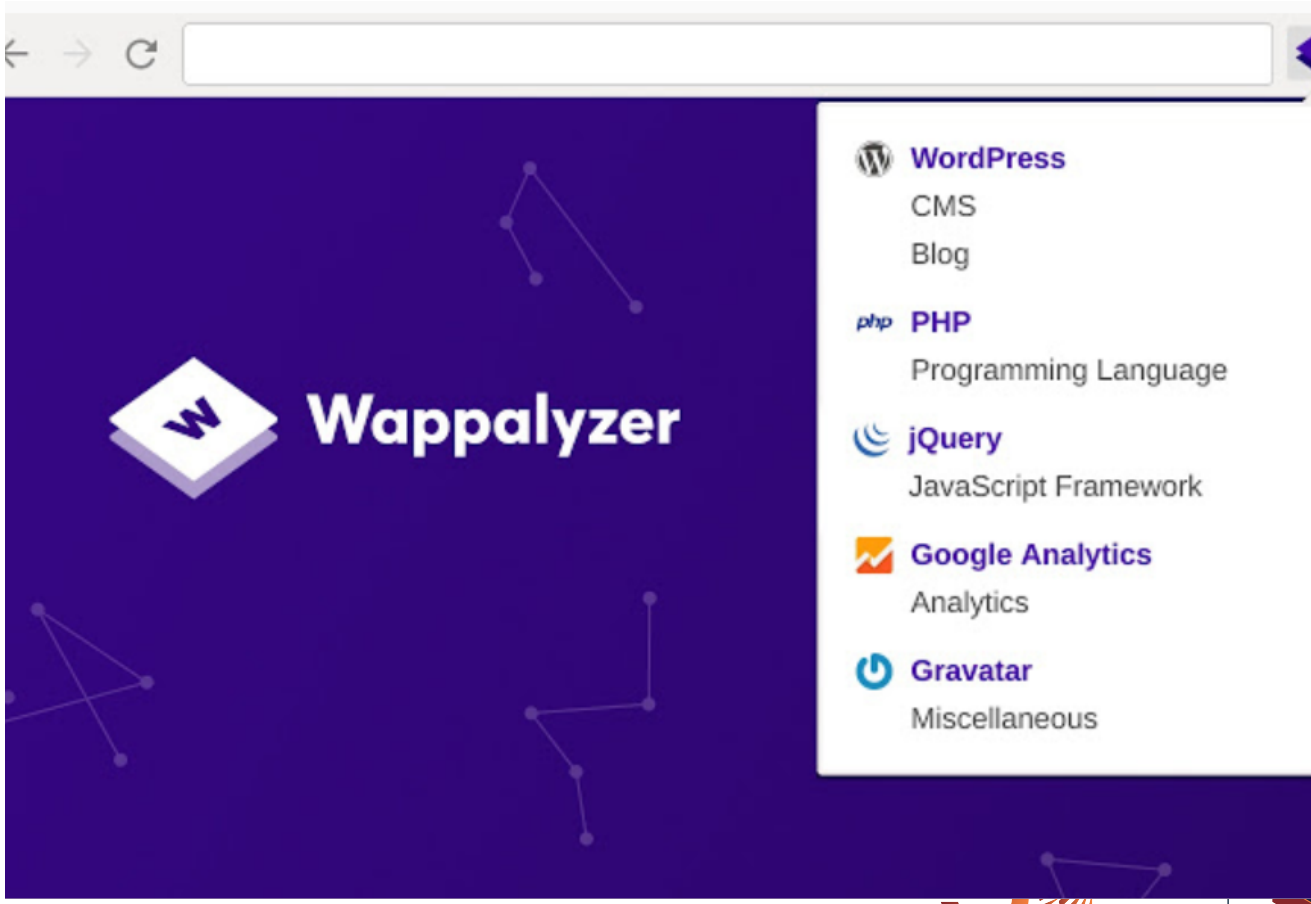


Wappalyzer.com

- **Download the tool, Install with firefox (add as plugin).**

Technologies Identified:

- **Frontend**
- **Backend**
- Wappalyzer is a **cross-platform utility that uncovers the technologies used on websites**. It detects content management systems, ecommerce platforms, web frameworks, server software, analytics tools and many more.
- It tells info related to wordpress, cms, PHP



DRILL

Select	Select one Website
Use	Use the above tools to find all the relevant information of selected website
Prepare	Prepare a report