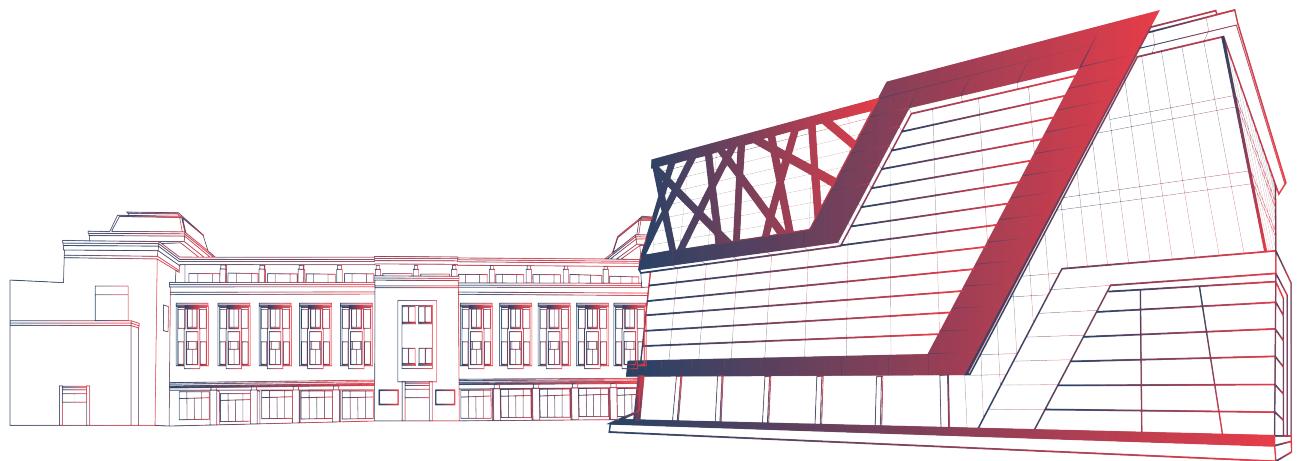


Information Gathering Basics & Tools



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.)

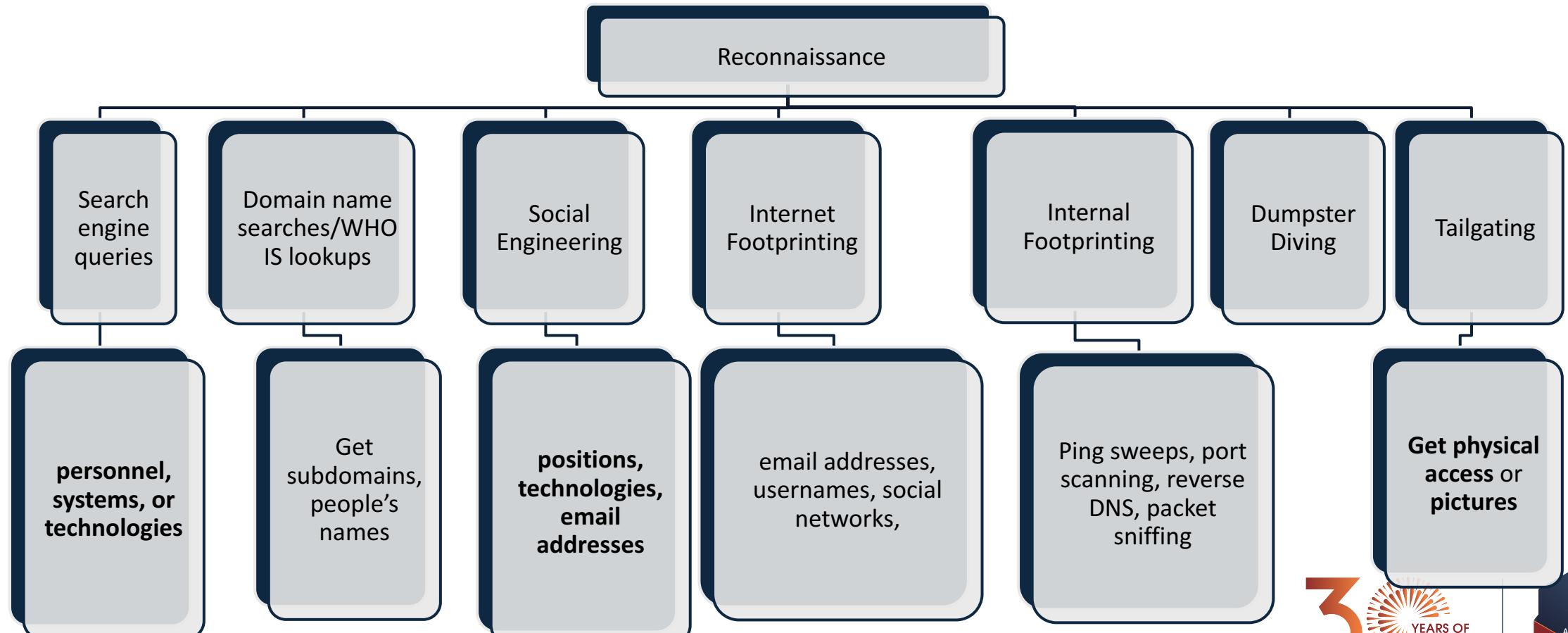
Information Gathering

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

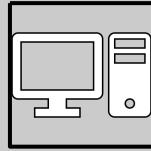
There's no need to break down the door to get inside when there **is a window open**.

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

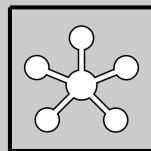
Common reconnaissance include



TYPES OF INFORMATION GATHERING



1. WEB BASED INFORMATION



2. NETWORK BASED INFORMATION GATHERING



3. INDIVIDUAL INFORMATION GATHERING



1. WEB BASED INFORMATION GATHERING :



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



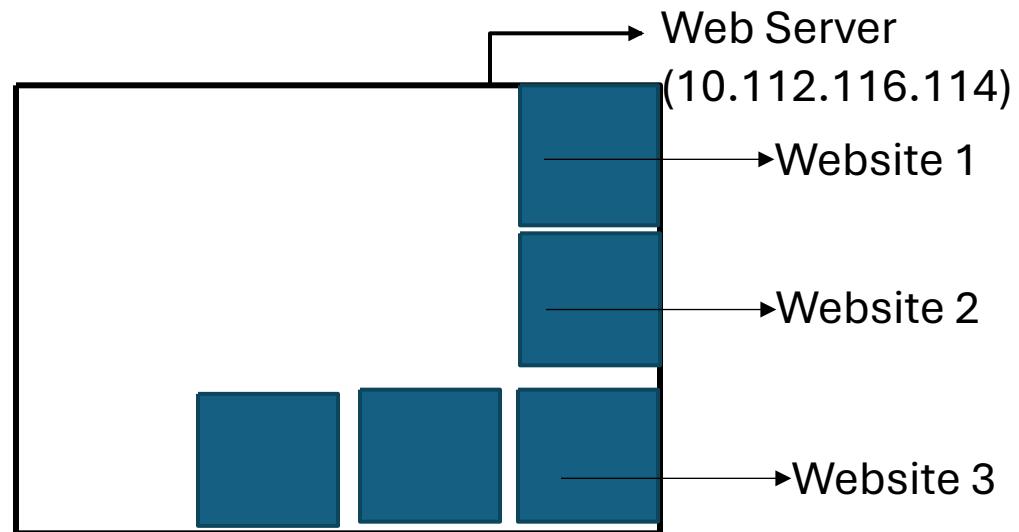
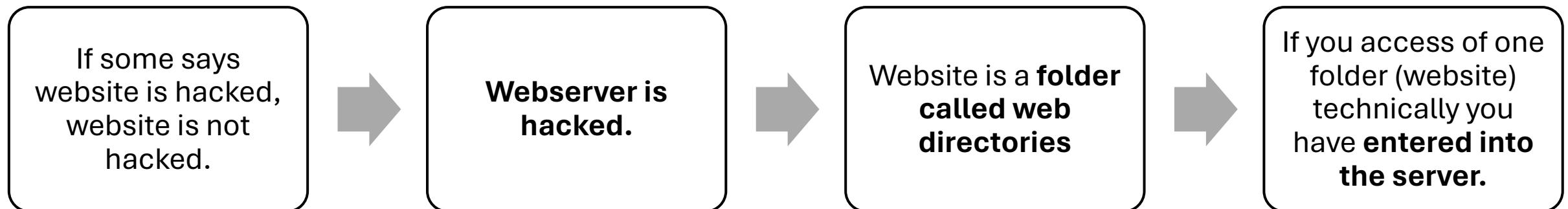
services of the Website it is using,
what are the **directories a Web Application** is having,
Server type whether it is using a **Shared Server or a Dedicated Server** etc.



Some Useful Tools -

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

To understand



Webservers

2 types of Web Servers

Shared Webservers

Dedicated Webservers

Shared Web servers

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**

Dedicated Web servers

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

Reconnaissance Tools

dnsstuff.com- <https://www.dnsstuff.com/>

Netcraft.com- [https://toolbar.netcraft.com/site report](https://toolbar.netcraft.com/site_report)

Yougetsignal.com- <https://www.yougetsignal.com/>

Whois.icann.org - <https://lookup.icann.org/>,

<https://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

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

Dnsstuff.com



The screenshot shows the homepage of tools.dnsstuff.com. At the top, there's a navigation bar with icons for home, lock, star, document, and search. The main header features the "DNSstuff" logo with "MANAGE | MONITOR | ANALYZE" below it. The IP address "160.202.39.61" is displayed. A SolarWinds logo is in the top right corner. Below the header, there are links for "Professional Toolset", "Mail Server Test Center", "Community", "Network Monitoring Software", and "Reviews". A horizontal menu bar includes "All Tools" (selected), "Domain/WWW Tools", "IP Tools", "Networking Tools", "Email Tools", and "Free Tools & Trials". The main content area is titled "Domain Tools" and contains six tool boxes: "DNSreport", "WHOIS/IPWHOIS Lookup", "See the smoke before you get burned" (an advertisement for SolarWinds ipMonitor), "WWW Co-host Tool", "Top Level Domain (TLD) Lookup", and "Abuse Lookup". Each tool box has a question and an input field with a blue "GO" button.



Dnsstuff.com- DNSReport

DNSreport

It generates report

It gives details of parent zone DNS servers

Records open DNS server

Generate Report & analyse- 5 mins Task

Dnsstuff.com- DNSReport

DNSreport Results for ncuindia.edu

Overall Results: 0 FAIL 4 WARNING 27 PASS 5 INFO

▼ PARENT

Status	Test Name	Information
WARN	Parent zone provides NS records	<p>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.</p> <pre>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</pre>
PASS	Number of nameservers	<p>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:</p> <pre>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</pre>

▼ NS

Dnsstuff.com-Whois Lookup

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.

Dnsstuff.com-Whois Lookup

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
+91 120 411 1000

Administrative Contact

Vijay Daulet-Singh
The National Capital University
HUDA Sector 23-A
+91 120 411 1000

Technical Contact

Deepak Satyarthi
The National Capital University
HUDA Sector 23-A
+91 120 411 1000



Tool 2

Netcraft

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

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



NETCRAFT

[Search...](#) 

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](#)



WWW.WEBAIR.COM
1.866.WEBAIR.1
SALES@WEBAIR.COM

[LEARN MORE ▶](#)

Netcraft Site Report

Lookup another URL:

Share:      

Background

Site title	Netcraft Internet Research, Anti-Phishing and PCI Security Services	Date first seen	January 1996
Site rank	3797	Primary language	English
Description	Not Present		
Keywords	Not Present		
Netcraft Risk Rating [FAQ]	0/10 		

Network

Site	http://www.netcraft.com	Netblock Owner	Amazon Technologies Inc.
Domain	netcraft.com	Nameserver	ns0.netcraft.com
IP address	52.85.201.229	DNS admin	hostmaster@netcraft.com
IPv6 address	Not Present	Reverse DNS	server-52-85-201-229.dub2.r.cloudfront.net
Domain registrar	networksolutions.com	Nameserver organisation	whois.networksolutions.com
Organisation	Statutory Masking Enabled, Statutory Masking Enabled, Statutory Masking Enabled, Statutory Masking Enabled, UK	Hosting company	Amazon



EXCELLENCE

Tool 3



Whois Lookup

You asking database whois to search

Who is this domain registered to?

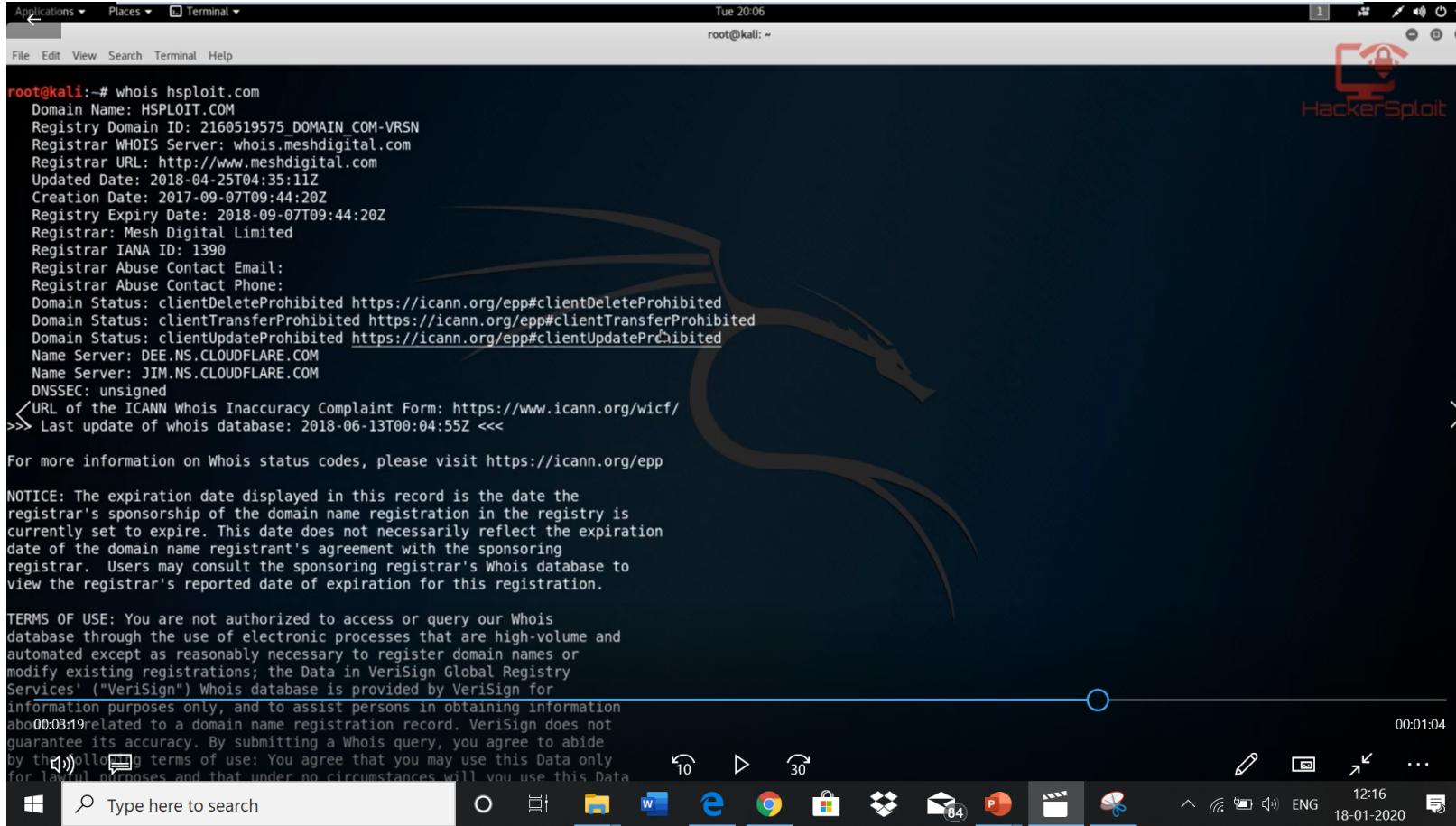
More details of the domain etc.

Can use this tool on Kali Linux

Command:

Whois hspolit.com

Whois



```

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

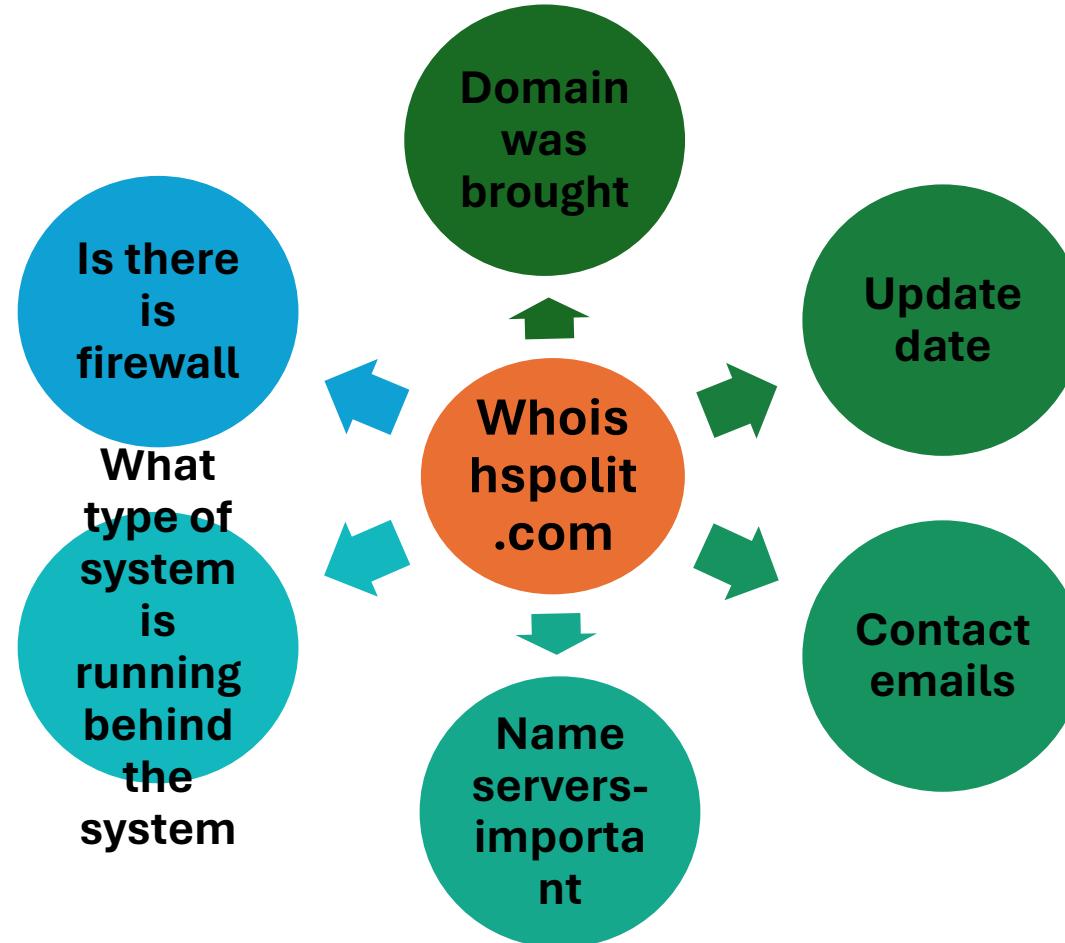
NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. 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 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
for lawful purposes, and that under no circumstances will you use this Data
for

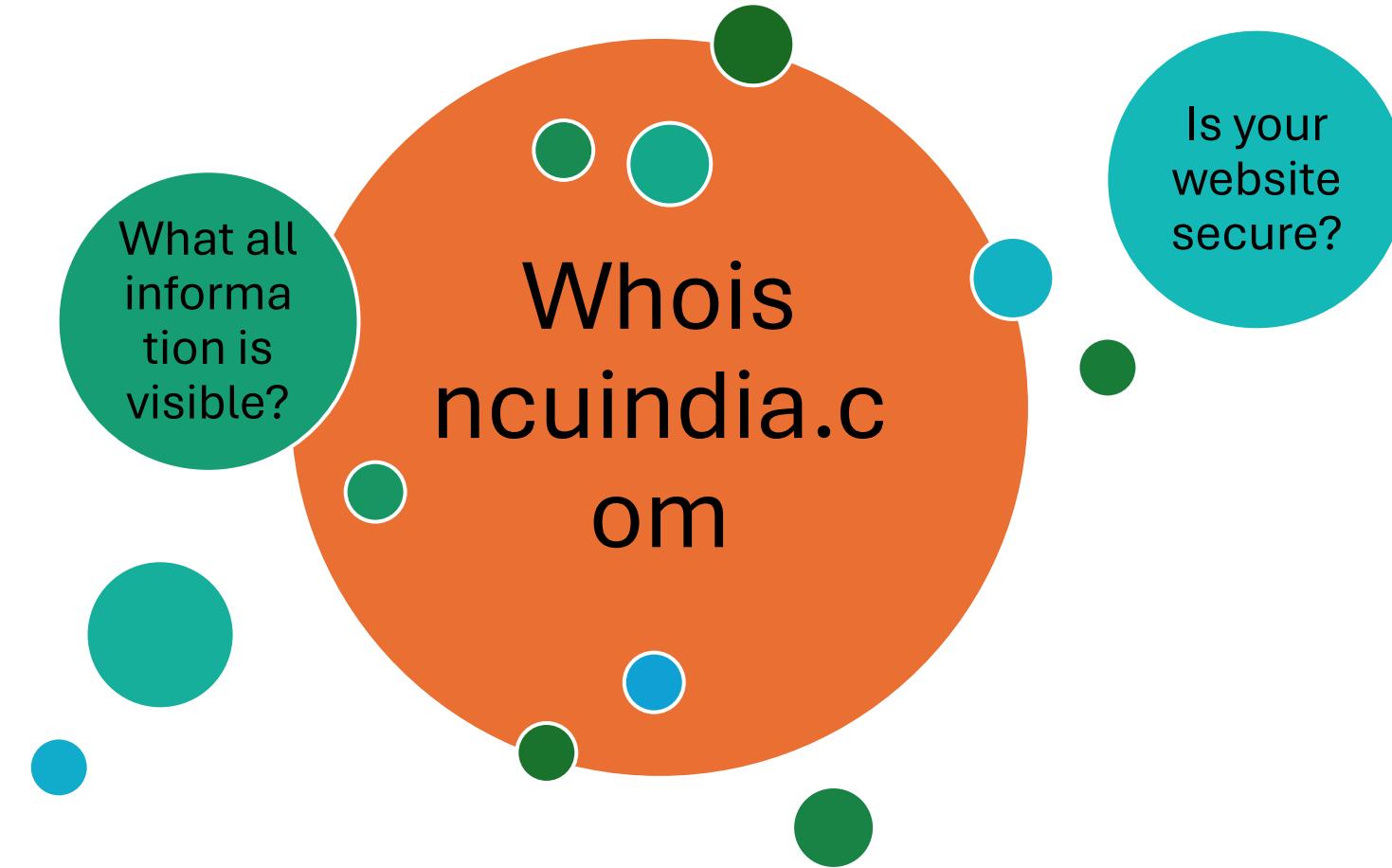
```



Whois Lookup



Whois task- 5 mins (kali Linux)



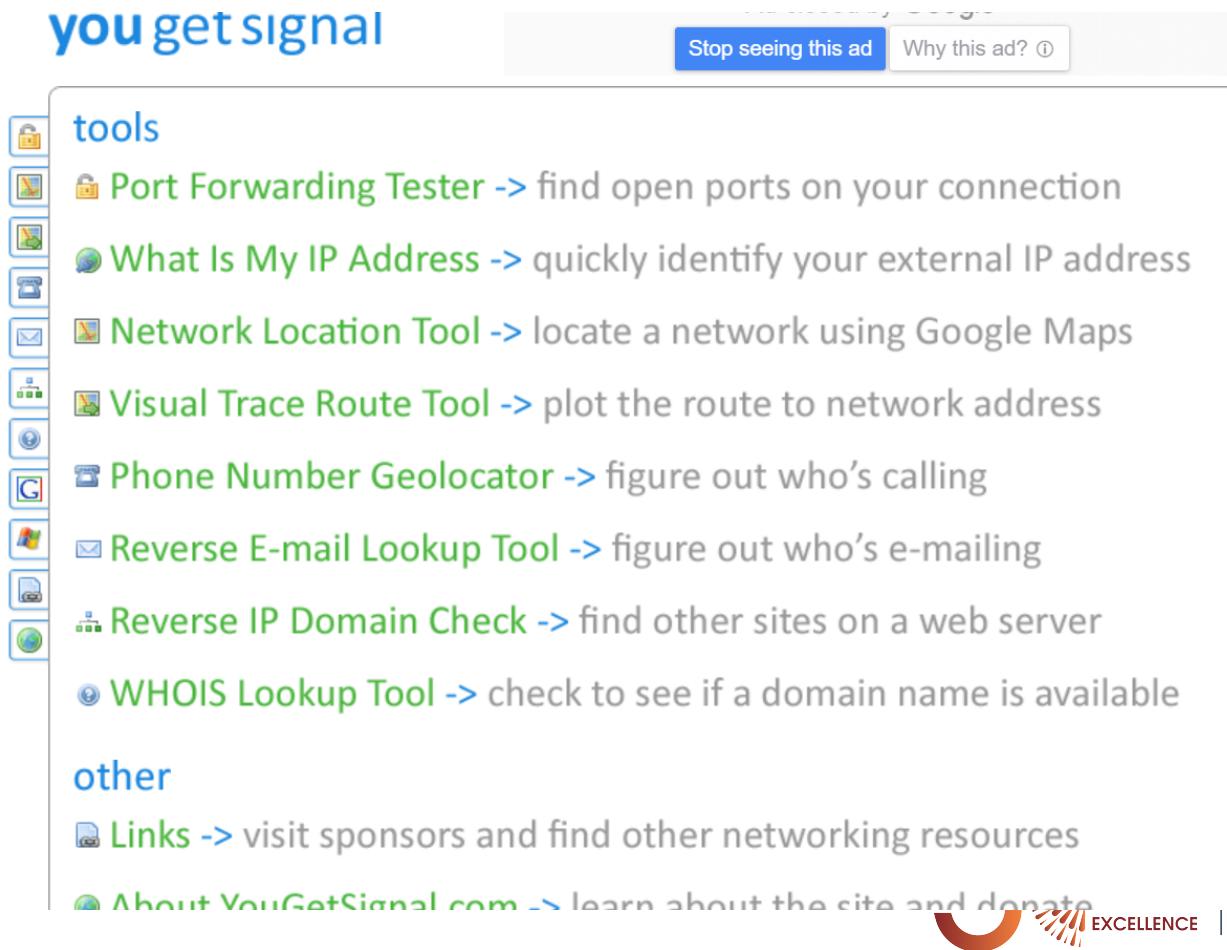
Tool 4



Yougetsignal.com (Tool)

Check many things online

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



The screenshot shows the homepage of YouGetSignal.com. At the top, there's a search bar with placeholder text "Search for something..." and a magnifying glass icon. Below the search bar is a navigation menu with items like "Home", "Tools", "About", "Links", and "Contact". The main content area has a light gray background with a white sidebar on the left containing icons for each tool category. The sidebar includes sections for "tools" and "other". Under "tools", there are eight items: "Port Forwarding Tester", "What Is My IP Address", "Network Location Tool", "Visual Trace Route Tool", "Phone Number Geolocator", "Reverse E-mail Lookup Tool", "Reverse IP Domain Check", and "WHOIS Lookup Tool". Under "other", there are two items: "Links" and "About YouGetSignal.com". At the bottom right of the page, there's a logo for NAAC Accredited and a banner that says "EXCELLENCE".

Yougetsignal.com (Tool) ->Reverse IP domain

Check number of domains and IP address of web server



Ad clos

Stop seeing thi

Reverse IP Domain Check



Remote Address

Find other sites hosted on a web server by entering a domain or IP address.

about

Note: For those of you interested, as of May 2014, my database has grown to over 10 million domains. You can purchase this [domain list for purchase](#).

A reverse IP domain check takes a domain name or IP address pointing to a web server and finds all other domains that can be hosted on that same web server. Data is gathered from search engine results, whois records, and the like. The Reverse IP Address.org provides interesting visual [reverse IP lookup tool](#). Knowing the other websites hosted on a single server is important from both an SEO and web filtering perspective, particularly for those on [shared web hosts](#). [More about this tool.](#) [Set an API Key.](#)

 help me pay for school (PayPal)



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)

Reverse IP Domain Check

Remote Address Check

Found 202 domains hosted on the same web server as [rakshittandon.com](#) (111.118.180.115).

It appears that the web server located at 111.118.180.115 may be hosting one or more web sites with explicit content. The web sites in question are highlighted in red below. There is a possibility that all of the web sites on this web server may be blocked by web filtering software. Search engine rankings for these web sites may be affected as well.

[aaagra.com](#)
[agrpublic.com](#)
[aioc2014.com](#)
[anandpistons.com](#)
[arenaagra.com](#)
[asthacity.com](#)
[bharatengine.com](#)
[bolticket.com](#)
[brakeshoemanufacturer.com](#)
[btcl.com](#)
[citizenpower.in](#)
[dasaprakashgroup.com](#)
[ektadairy.com](#)
[farry.in](#)
[fhmc.co.in](#)
[fishcopfed.in](#)
[gayatridevelopwell.com](#)
[gle1845.com](#)
[guiderammital.com](#)
[haridarshan.com](#)
[herbalgulal.net](#)
[hoteldeluxplaza.in](#)
[icpr.org](#)
[innovativesystemsindia.com](#)
[jinvanichannel.com](#)
[khabarexpert.com](#)
[labriza.com](#)
[livetv.jinvanichannel.com](#)
[mangalayatan.in](#)
[midnightbazar.in](#)
[omsshirerealtech.com](#)
[opchainsltd.com](#)
[ozimports.net](#)
[panchipetha.in](#)
[pavnasports.com](#)
[popularfoodsindia.com](#)
[qacertification.asia](#)
[raavievents.com](#)
[rakshittandon.com](#)
[rbitagra.org](#)

[aapkajawab.in](#)
[agrpublicschool.com](#)
[ajebs.com](#)
[anilahenna.com](#)
[arinfosec.com](#)
[basantoil.com](#)
[bing.com](#)
[brakedrumsindia.com](#)
[brijeshpix.com](#)
[certificationsindia.com](#)
[cybercellagra.com](#)
[derbyfootwear.com](#)
[enhancebuildtech.com](#)
[fashiontantra.in](#)
[fhmc.in](#)
[flywheelassembly.com](#)
[gayatrimart.com](#)
[gplus.in](#)
[guptaoverseas.com](#)
[helpagra.com](#)
[hotelbhawnapalace.com](#)
[hotellkamal.com](#)
[iifa-india.com](#)
[itmaliigarh.com](#)
[kamayanihospital.com](#)
[khannaautomart.com](#)
[live.jinvanichannel.com](#)
[mangalayatan.com](#)
[mgresidency.com](#)
[neelamcollege.com](#)
[opchainshousings.com](#)
[ozcleaningservices.net](#)
[ozsecurity.net](#)
[panchipetha.com](#)
[photopixel.in](#)
[ppdcagra.in](#)
[qualitytestingequipment.com](#)
[rainbowinfrahousing.com](#)
[rbcolour.com](#)
[remotetechsupports.com](#)



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)

Tool 5



whois.icann.org (search on google)

Whois.icann.org

ICANN (father) Non-profitable org

IANA (Son)-paid

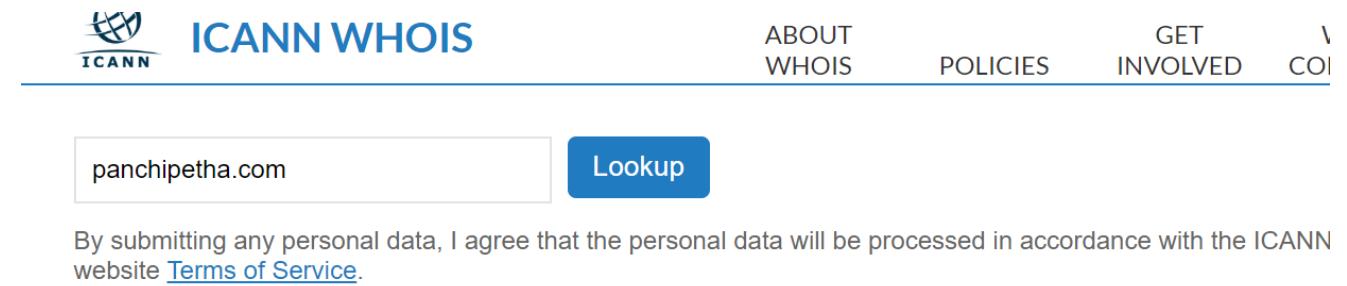
Domain is provided by

Service Provider (Godaddy.com)

Whois.icann.org

Can see the details of website

- E.g. panchipetha.com



The screenshot shows the ICANN WHOIS search interface. At the top, there's a logo for ICANN and the text "ICANN WHOIS". Below that is a search bar containing "panchipetha.com" and a blue "Lookup" button. To the right of the search bar, there are links for "ABOUT WHOIS", "POLICIES", "GET INVOLVED", and "COI". Below the search bar, a message states: "By submitting any personal data, I agree that the personal data will be processed in accordance with the ICANN website [Terms of Service](#)".

Showing results for: panchipetha.com

Original Query: panchipetha.com

Contact Information

Registrant Contact

Name: Ankit Goyal
Organization: NA
Mailing Address: 15-343
Noorigate, Agra Uttar Pradesh

Admin Contact

Name: Ankit Goyal
Organization: NA
Mailing Address: 15-343
Noorigate, Agra Uttar Pradesh

Tech Contact

Name: Ankit Goyal
Organization: NA
Mailing Address: 15-343
Noorigate, Agra Uttar Pradesh



Whois.icann.org

- Can see the details of website
- E.g. Lucideus.com
- **No information is revealed**

Whois Record for LuceDioUs.com

Domain Available



lucedious.com is for sale!

The domain you are researching is available for registration.

[Buy lucedious.com](#)

— Domain Profile

Domain Status Never Registered Before

— Website

Website Title None given.

Whois Record

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 Used Configure Router Settings

July 06, 2016 by 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.

 DOMAINTOOLS PROFILE ▾ CONNECT ▾ MONITOR ▾ SUPPORT Whois Lookup

Whois Record for nCulndia.edu

— Domain Profile

Registrant Org	The National Capital University
Registrar Status	
Dates	1,472 days old Created on 2015-05-26 Expires on 2019-07-31 Updated on 2019-04-26
Tech Contact	Deepak Satyarthi
IP Address	35.154.226.226 is hosted on a dedicated server
IP Location	 - Maharashtra - Mumbai - Amazon Data Services India
ASN	 AS16509 AMAZON-02 - Amazon.com, Inc., US (registered May 04, 2000)
Hosting History	2 changes on 3 unique name servers over 4 years

— Website

Website Title	 Top University in Delhi NCR, India - The NorthCap University
---------------	--

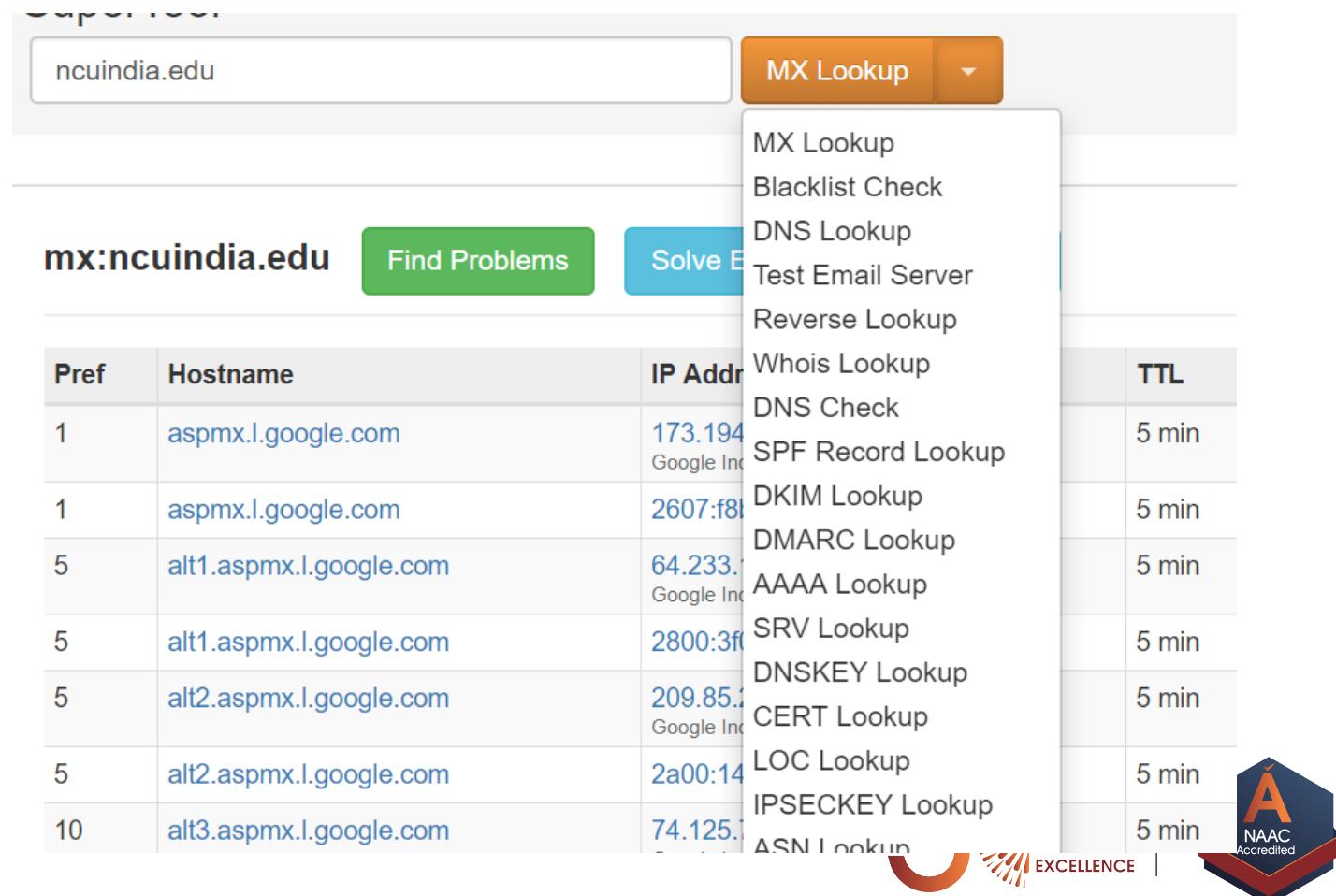


Tool 6,7,8,9



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



The screenshot shows the Mxtoolbox.com interface. At the top, there is a search bar with "ncuindia.edu" and a dropdown menu labeled "MX Lookup". Below the search bar, there is a sub-navigation bar with "mx:ncuindia.edu", "Find Problems", and "Solve Email Problems". A dropdown menu is open over the "MX Lookup" button, listing various lookup options: MX Lookup, Blacklist Check, DNS Lookup, Test Email Server, Reverse Lookup, Whois Lookup, DNS Check, SPF Record Lookup, DKIM Lookup, DMARC Lookup, AAAA Lookup, SRV Lookup, DNSKEY Lookup, CERT Lookup, LOC Lookup, IPSECKEY Lookup, ASN Lookup, and ASN Lookup. To the right of the dropdown, there is a table showing MX records for "ncuindia.edu". The table has columns for "Pref", "Hostname", "IP Address", and "TTL". The TTL column shows values of 5 min for all entries. The table data is as follows:

Pref	Hostname	IP Address	TTL
1	aspmx.l.google.com	173.194.67.10 Google Inc.	5 min
1	aspmx.l.google.com	2607:f8b0:4e1::d Google Inc.	5 min
5	alt1.aspmx.l.google.com	64.233.112.12 Google Inc.	5 min
5	alt1.aspmx.l.google.com	2800:3f0:1000::d Google Inc.	5 min
5	alt2.aspmx.l.google.com	209.85.140.12 Google Inc.	5 min
5	alt2.aspmx.l.google.com	2a00:1400:1000::d Google Inc.	5 min
10	alt3.aspmx.l.google.com	74.125.100.12 Google Inc.	5 min

Ip2location.com

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

[Share The Result](#)

https://www.ip2location.com/203.115.107.67

03.115.107.67

 India [IN] ⓘ

Haryana

Gurgaon

8.466670, 77.033330 (28°28'0"N 77°1'60"E)

tm Sec 23 Gurgaon

6 Jun, 2019 01:19 PM (UTC +05:30)

rimenet.in

COMP) Company/T1

91) 0124

Multilingual

IP2Location provides free multilingual data of country, region and customers to download.

Continent Names	Asia (EN), آسیا (EL), ಏಷ್ಯಾ (KM), アジア (LO) & 75 more...
Country Names	India (EN), ભારત (KN), ຖ්‍රුක් (BO), In Indie (PL) & 75 more...
Region Names	Haryana (EN), حارہن (AR), Haryana (Haryana (ET) & more...
City Names	ગुರगांव (HI)
Region Code	10

Tools/Utilities

You can easily lookup an IP address on the below channels using t

Twitter Bot	@ip2location 203.115.107.67
Slack Bot	/ip2location 203.115.107.67
Monitor ⓘ	



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**

Nameservers: mumapps2.primenet.in >> 203.115.112.86
delapps1.primenet.in >> 203.115.96.85

Location For IP: 203.115.107.67

Continent: Asia (AS)

Country: India  (IN)

Capital: New Delhi

State: Haryana

City
Location: Gurgaon

Postal: 122002

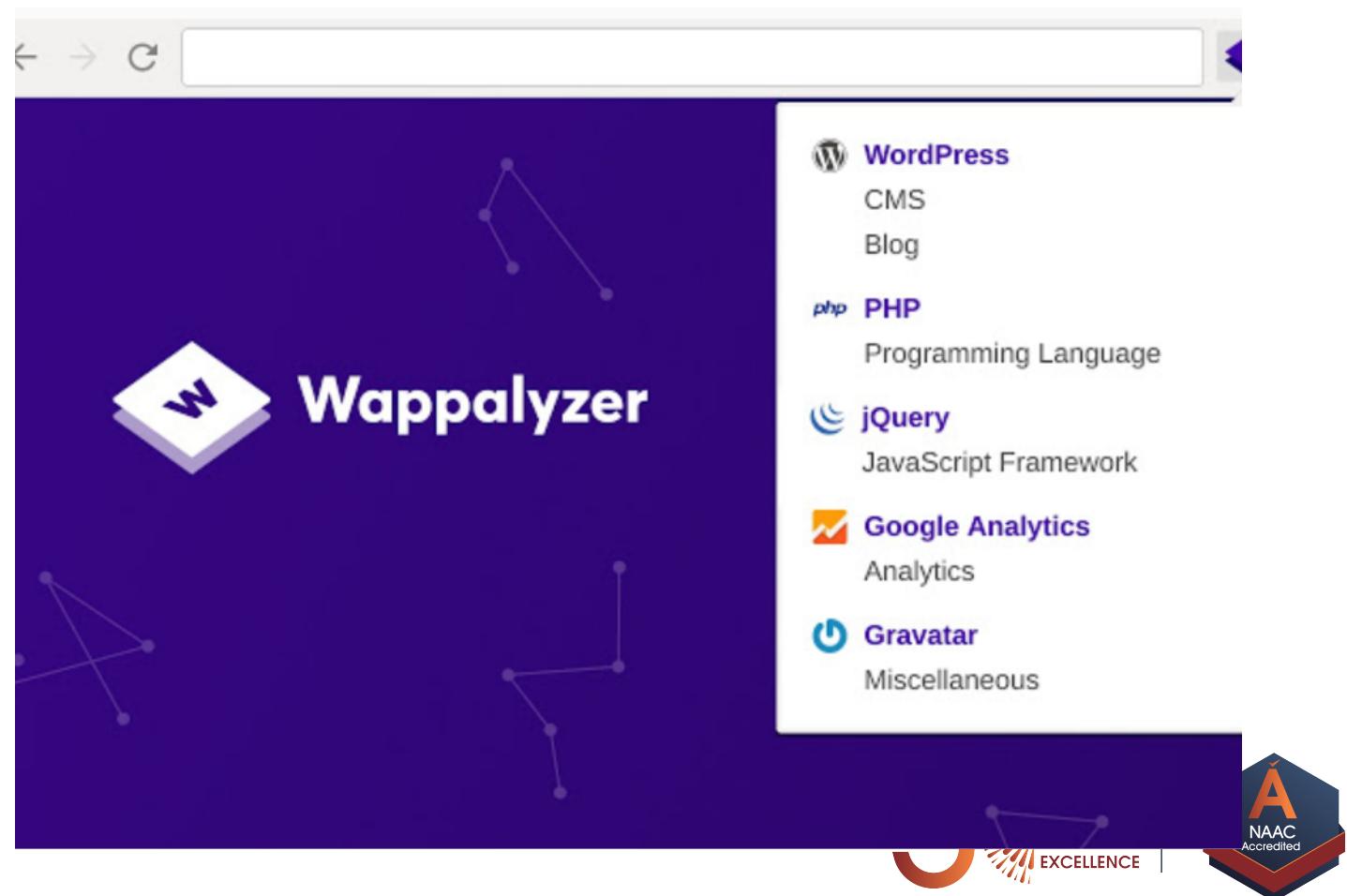
ISP: Primenet Global

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

