****

****

**What’s information gathering?**

When it comes to getting a clear information gathering concept, the simplest way to define it would be the process of collecting information about something you are interested in. A practical example: gathering information with your eyes is called visual perception. In the same way, in the digital world, a lot of information can be gathered in different ways, not with your senses, but with several methods, tools and techniques.

For those in the cybersecurity industry, this is the first step to take during the earlier stages of any hacking activity (both [cracking](https://securitytrails.com/blog/hacker-vs-cracker#what-is-a-cracker) and [ethical hacking](https://securitytrails.com/blog/ode-white-hats-ethical-hacking)), when any black- or white-hat researcher needs to **gain as much information as possible about the desired target**.

While it’s a fun activity for some researchers, information gathering is also one of the most time-consuming tasks during the intel-recon process, and that is why time management is so important.

What are the objectives of information gathering in cybersecurity?

Any basic cybersecurity information gathering process often includes these two types of data collection goals:

1. Collecting network data: Such as public, private and associated domain names, network hosts, public and private IP blocks, routing tables, TCP and UDP running services, SSL certificates, [open ports](https://securitytrails.com/blog/open-ports) and more.
2. Collecting system-related information: This includes user enumeration, system groups, OS hostnames, OS system type (probably by [fingerprinting](https://securitytrails.com/blog/cybersecurity-fingerprinting)), system banners (as seen in the [banner grabbing](https://securitytrails.com/blog/banner-grabbing) blog post), etc.

But there’s a lot more involved. Let’s learn about it, by exploring the most popular techniques used during this phase.

INFORMATION GATHERING METHODOLOGY

1. Find out initial information like IP address, domain name and open-source information.
2. Find out address range of the network.
3. Find active machines
4. Find open ports or access point (Ports are the door and windows of the system that an intruder uses to gain access using port scanning. ports scanner is a program that an attacker would use to determine which port are open on the system)
5. Figure out the open system)
6. Figure out which service are running on each port. (Knowing Which specific service is running enables the attacker to look up exploit and launch known vulnerabilities against the service)
7. Map out the network (after gathering as much information as possible, an attacker will figure out what to do with the network. An attacker can use trace route or ping or some automated programs to find out the information for mapping the network)

Active Information Gathering

In active information gathering , there is direct interaction with the target, for example , gathering information about what port are open on a particular target , what service they are running and What operating system is being used. Active information gathering techniques can be easily detected by IDS, IPS, and firewalls and generate a log of presence.

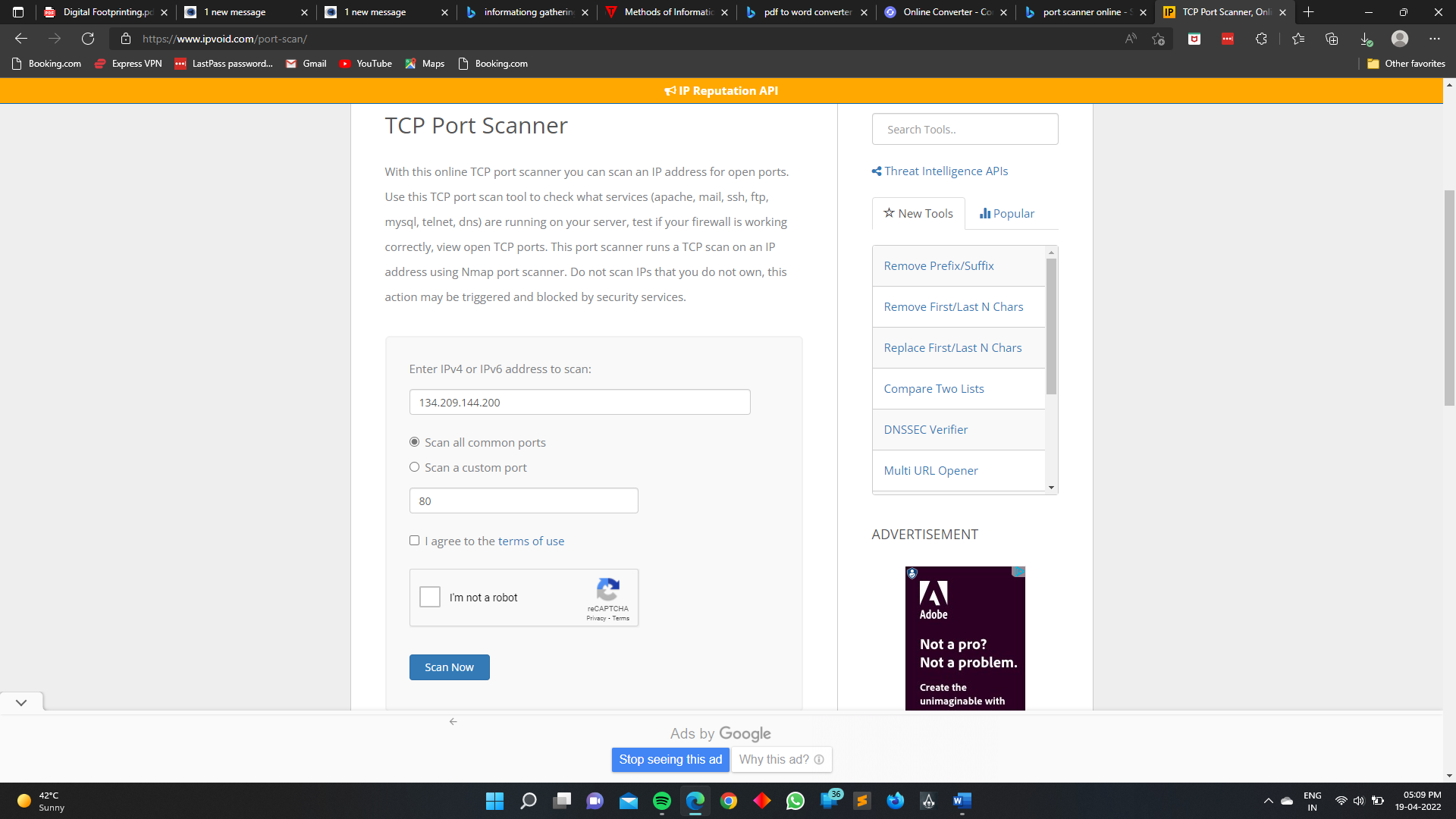
Passive Information Gathering

In passive information gathering information is collected without establishing contact with the target. This is pre-attack phase for gathering information like what system a victim is using , what software are installed is their systems , network range , active machines, open ports etc. theHarvester , netcraft, Maltego etc.are some tools used for passive information gathering.

INFORMATION GATHERING THROUGH WEBSITE

Website [TCP Port Scanner, Online Port Scan, Port Scanning | IPVoid](https://www.ipvoid.com/port-scan/)

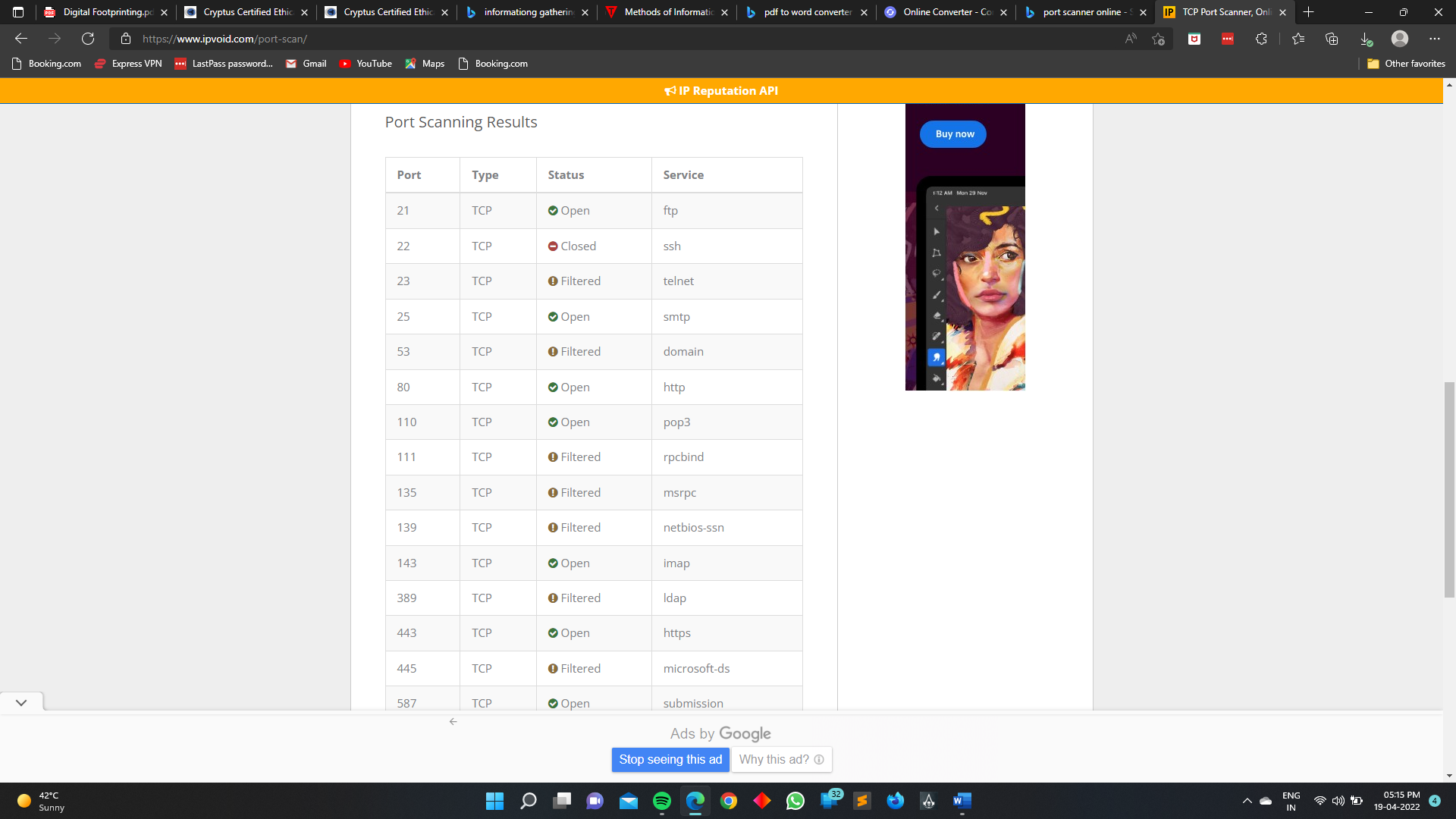
(for port scanning)



Here I am using the Ip address of cryptus for testing the ports of the website .

Select the Scan all the ports.

I agree to the terms of use.



Here we see all the open and close port of website…

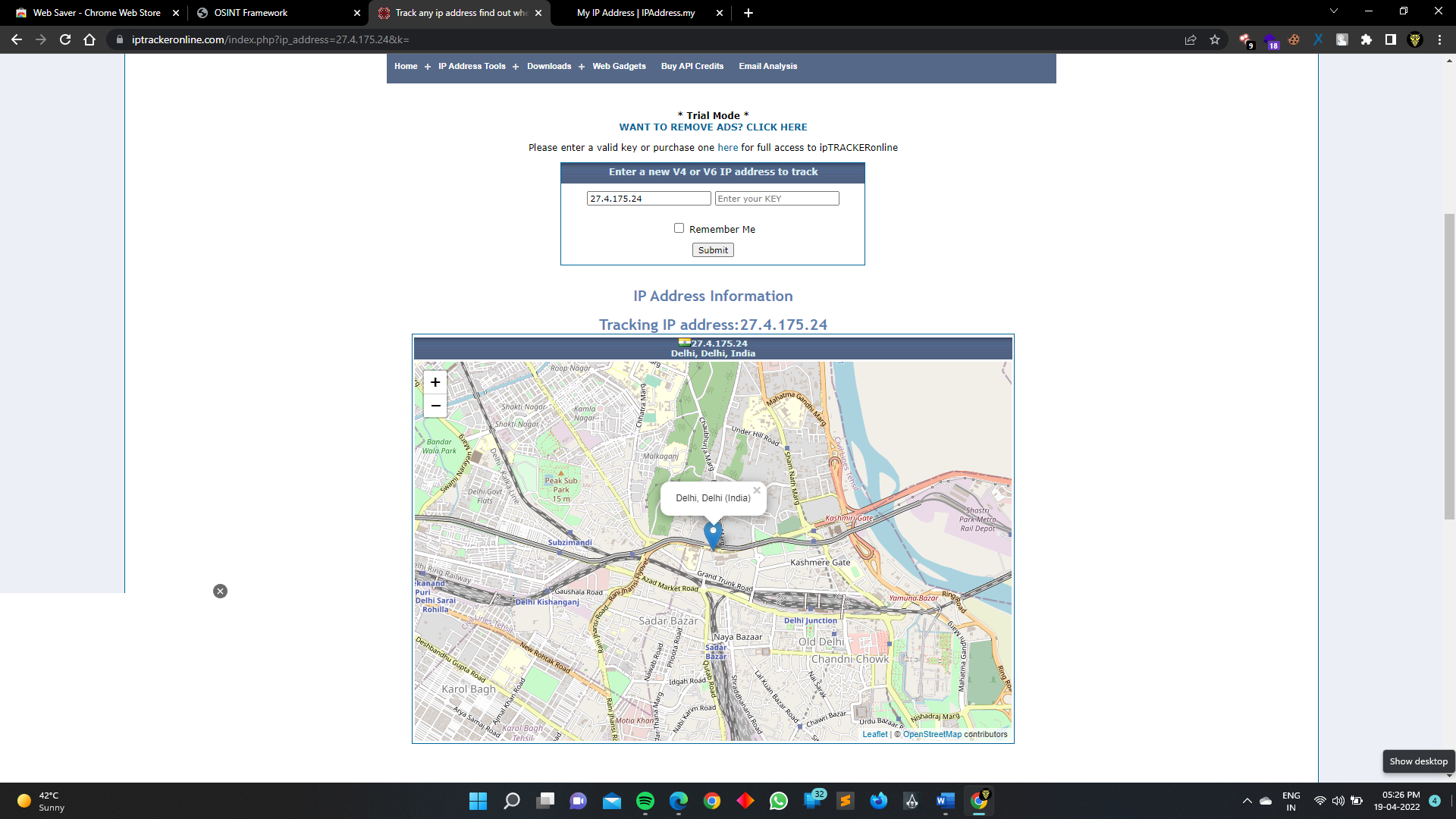
Open

Closed

Filtered

What is IP Geo Location

IP geo location is the mapping of an ip address to the geographic location of the internet from the connected device. It provides location information such as the country, sate, zip code, latitude/longitude , ISP , area code, and other information.

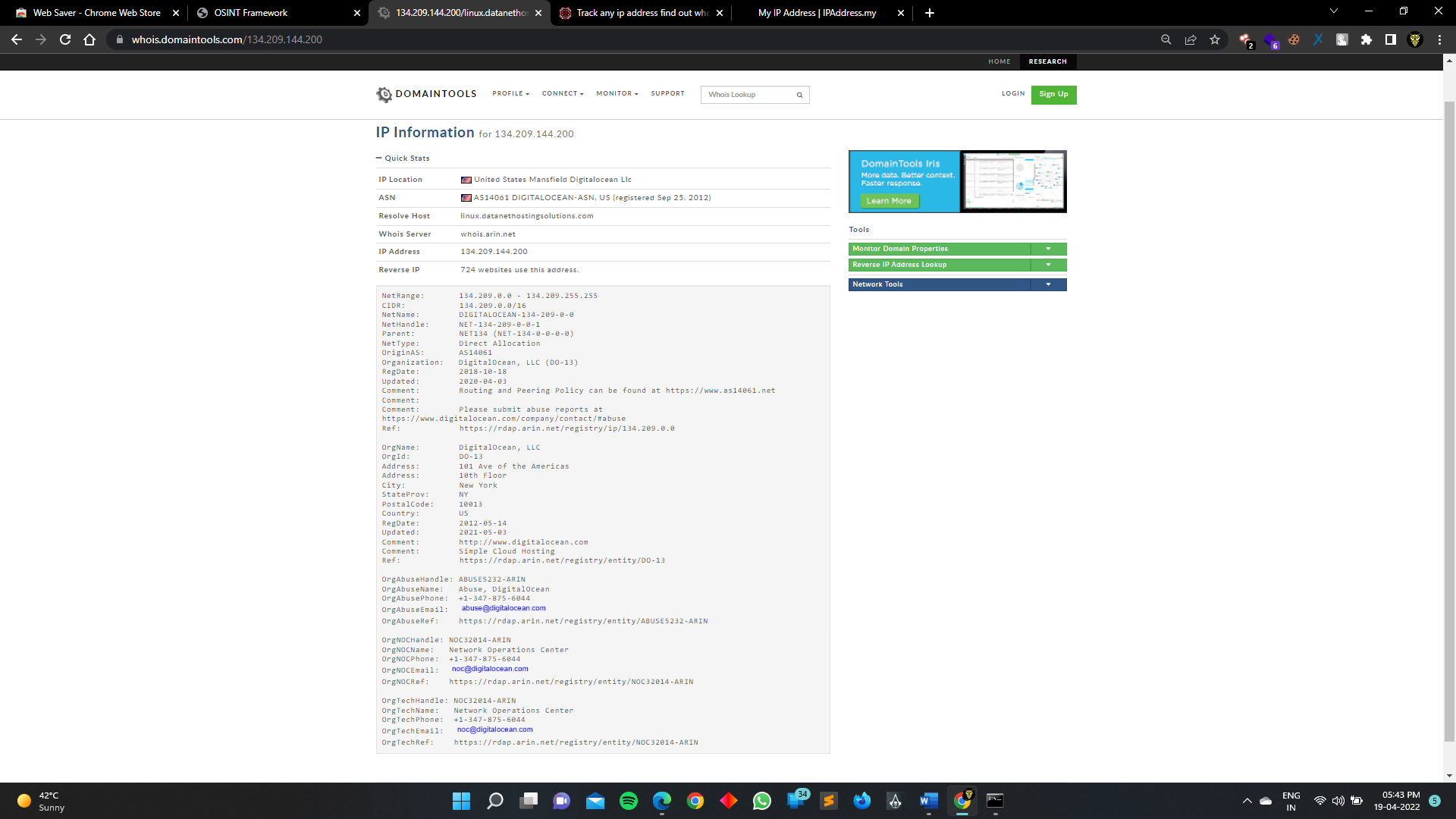


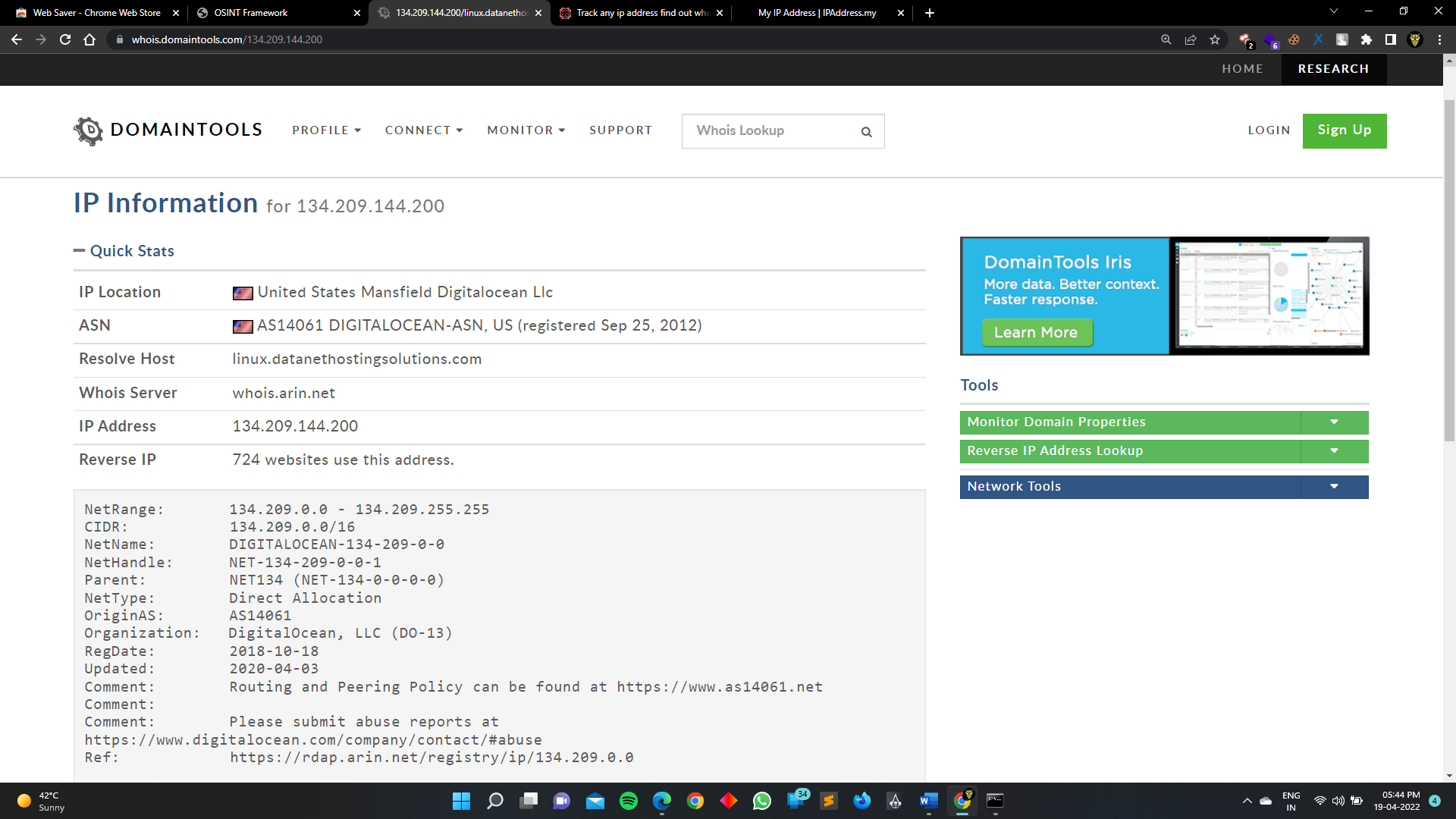
Website :- <https://www.iptrackeronline.com/>

With the help of this website you can easily see the location of you target..

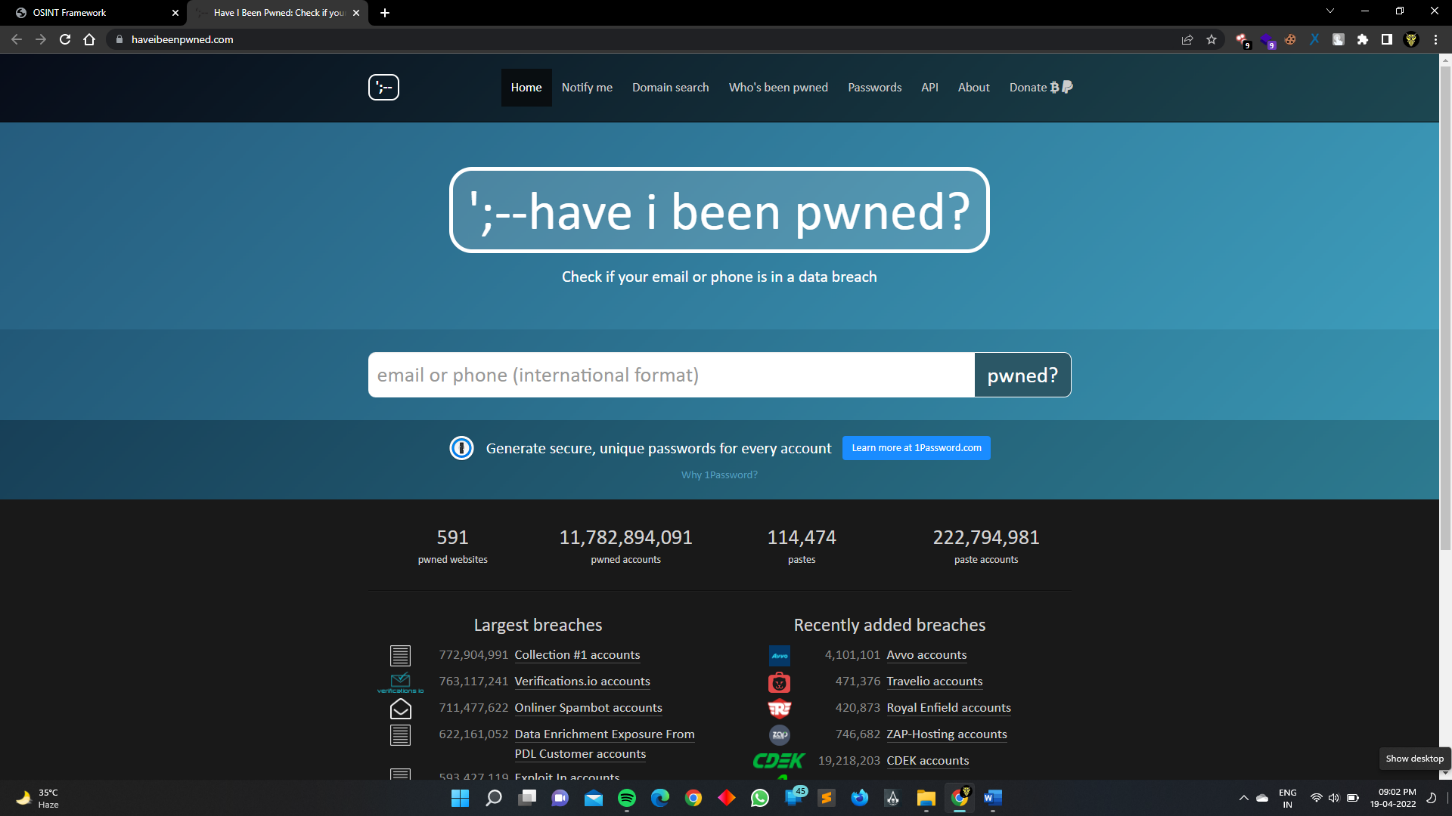
Who is Lookup (Tools)

WHOIS (pronounced as the phrase "who is") is a query and response protocol that is widely used for 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





Have I Been Pawned

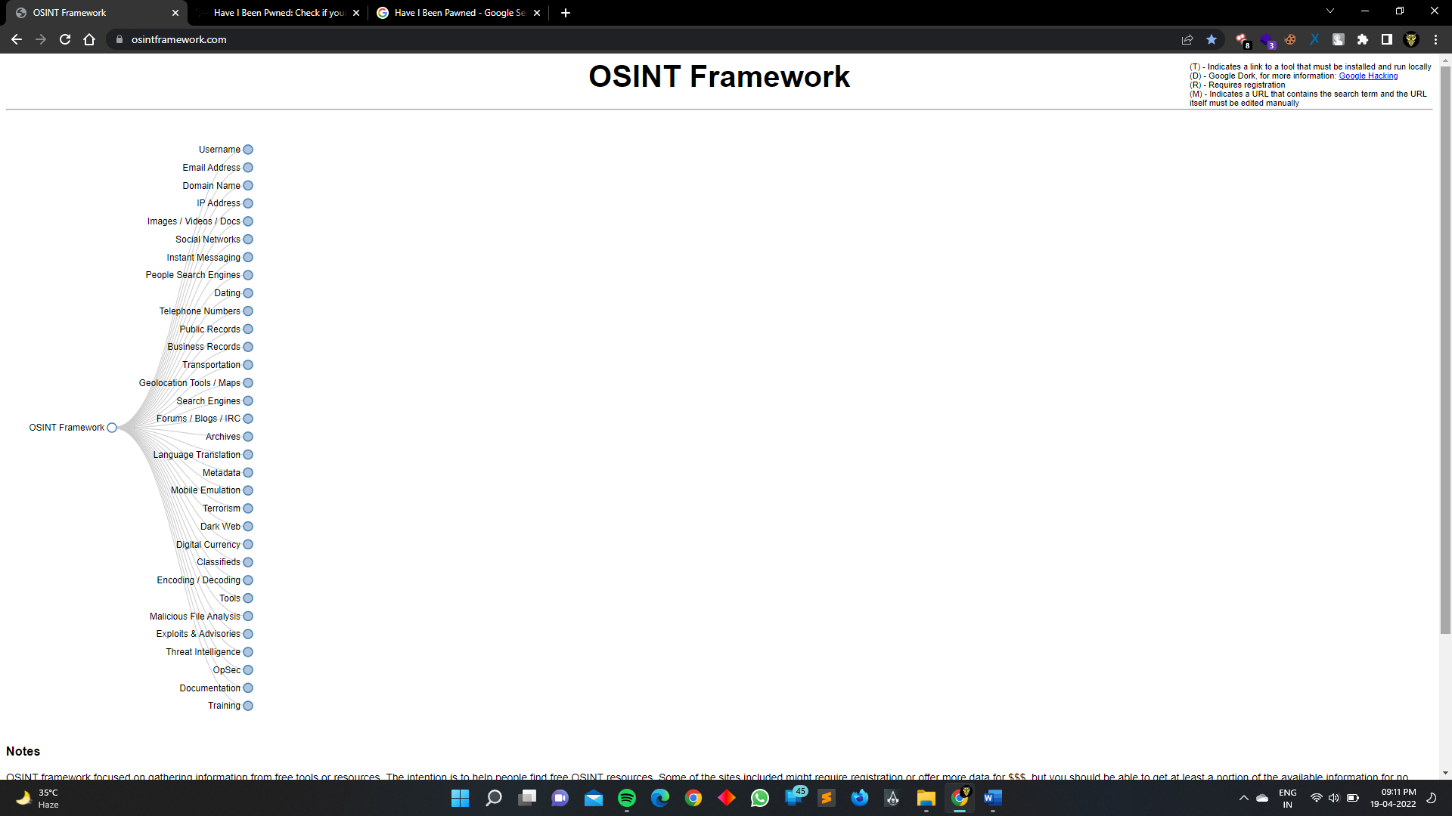


Website :- <https://haveibeenpwned.com/>

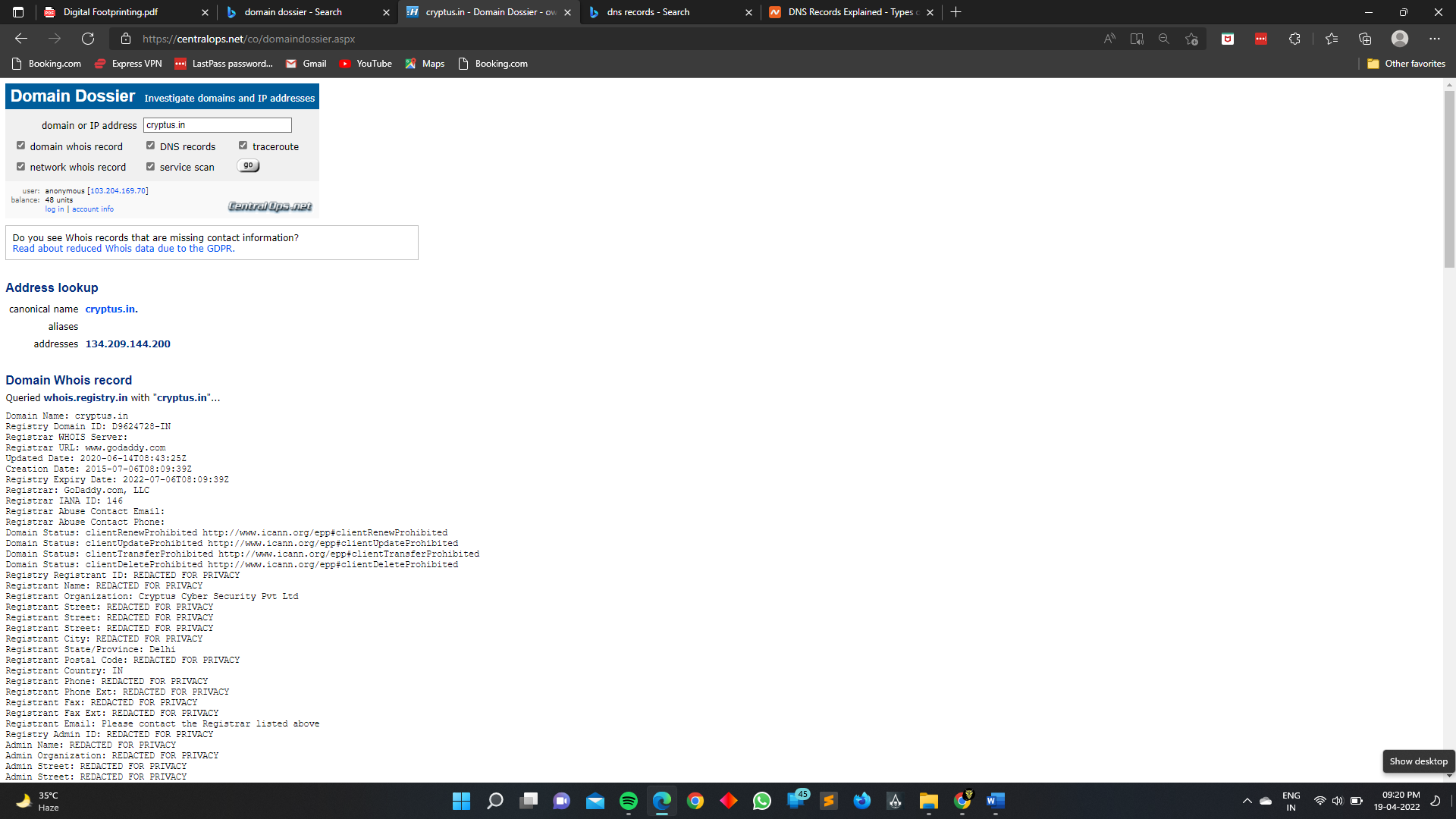
Have I Been Pawned? is a website that allows Internet users to check whether their personal data has been compromised by data breaches

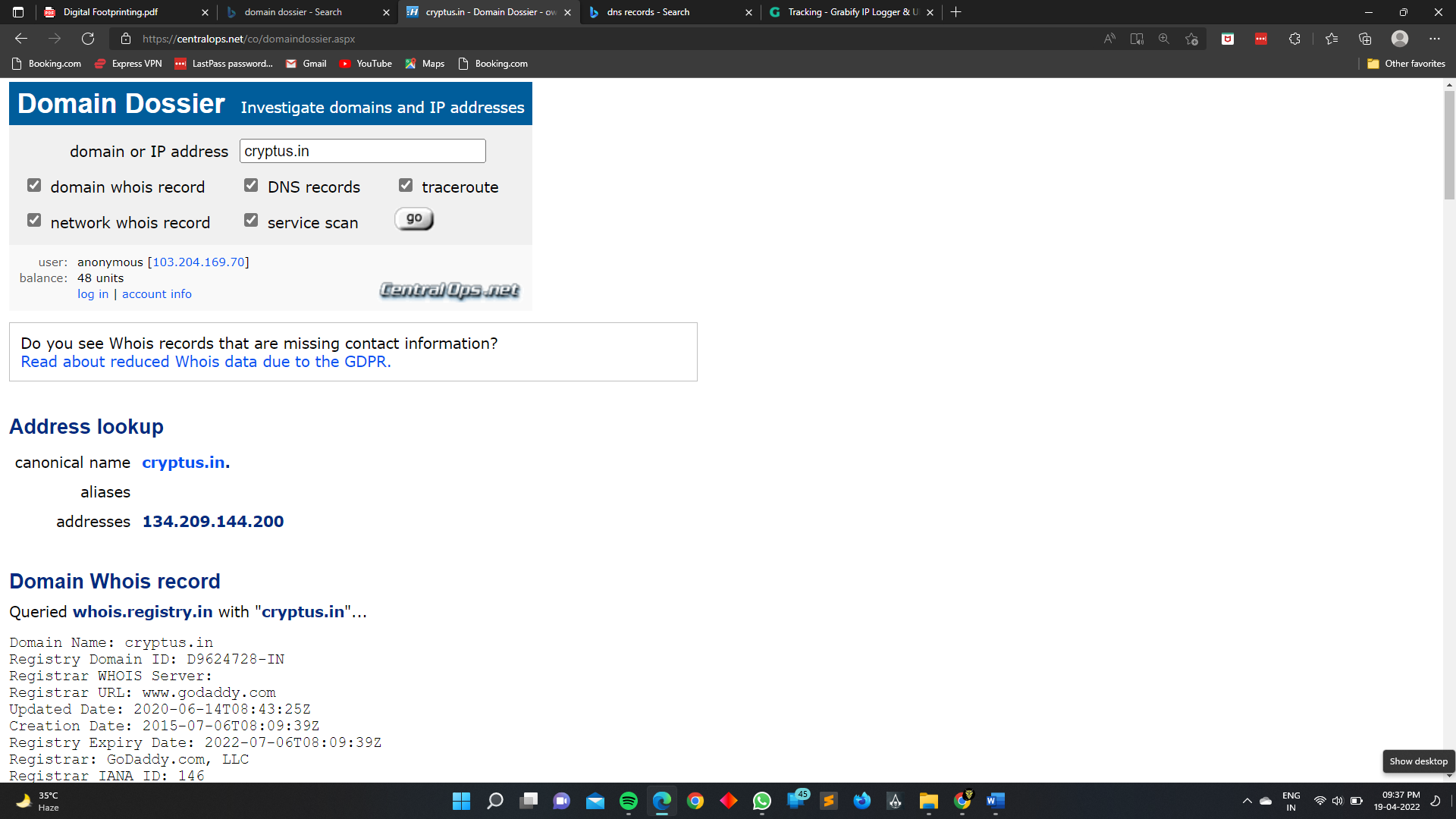
**OSINT Framework**

OSINT Framework, as its name implies, is **a cybersecurity framework, a collection of OSINT tools to make your intel and data collection tasks easier**. This tool is mostly used by security researchers and penetration testers for digital foot printing, OSINT research, intelligence gathering, and reconnaissance



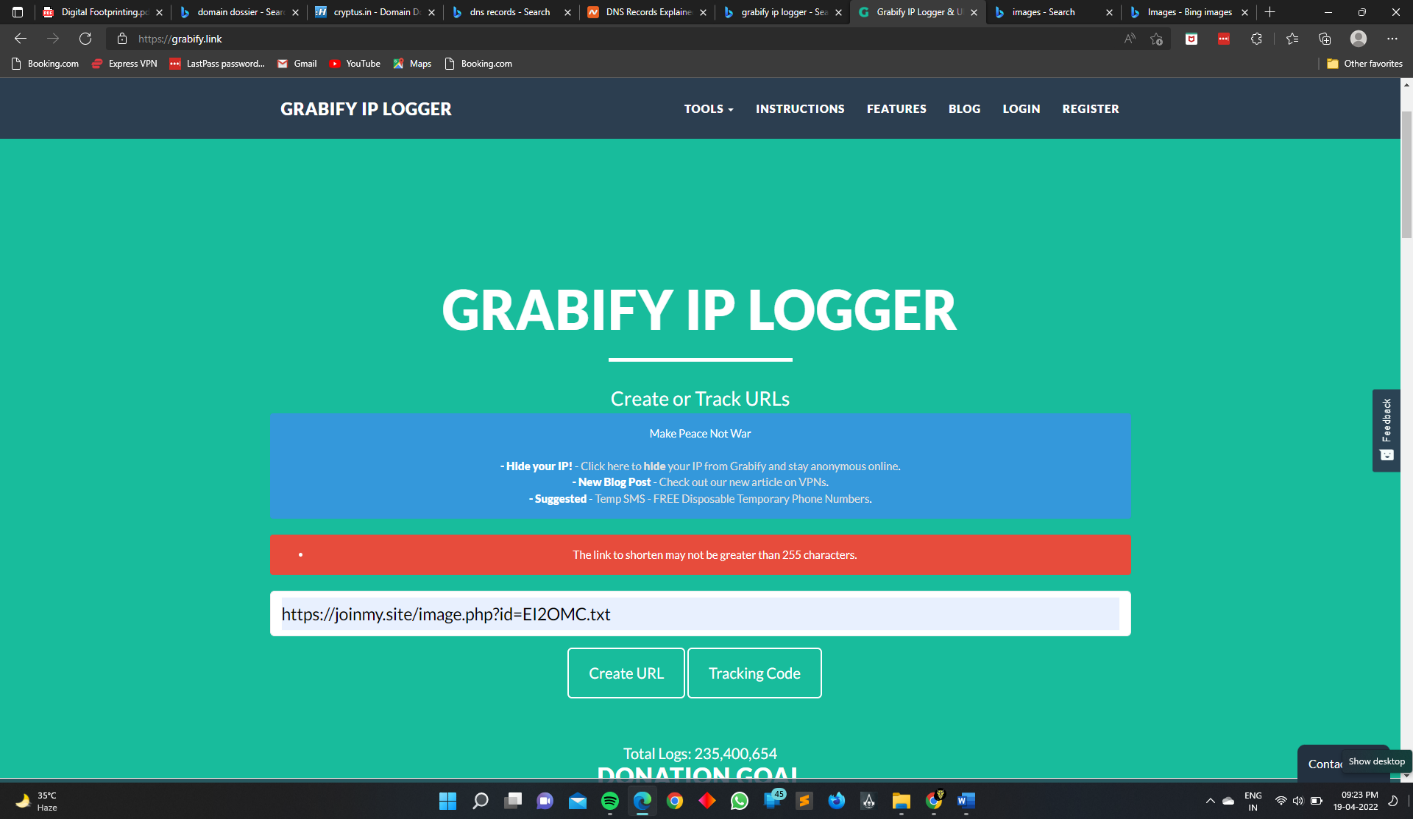
Domain Dossier (Investigate domains and IP addresses)



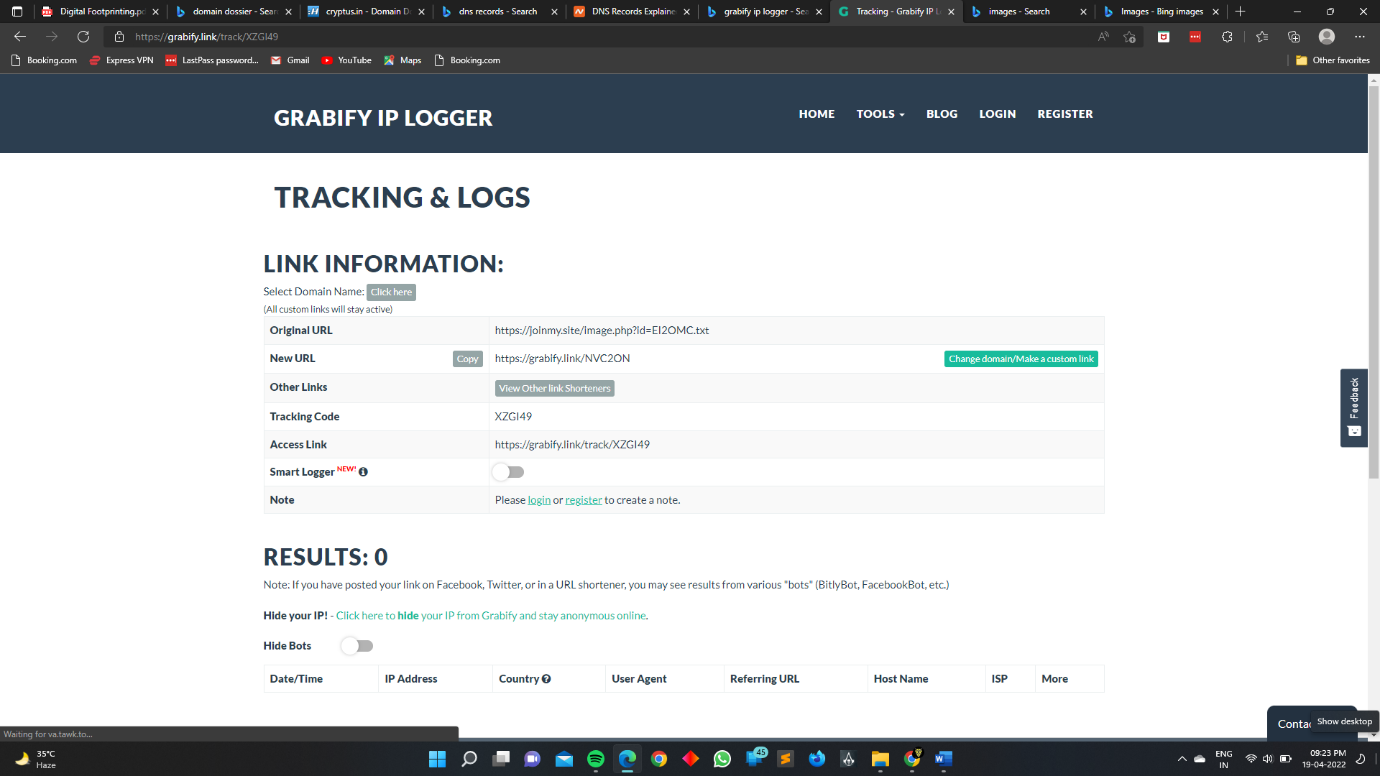


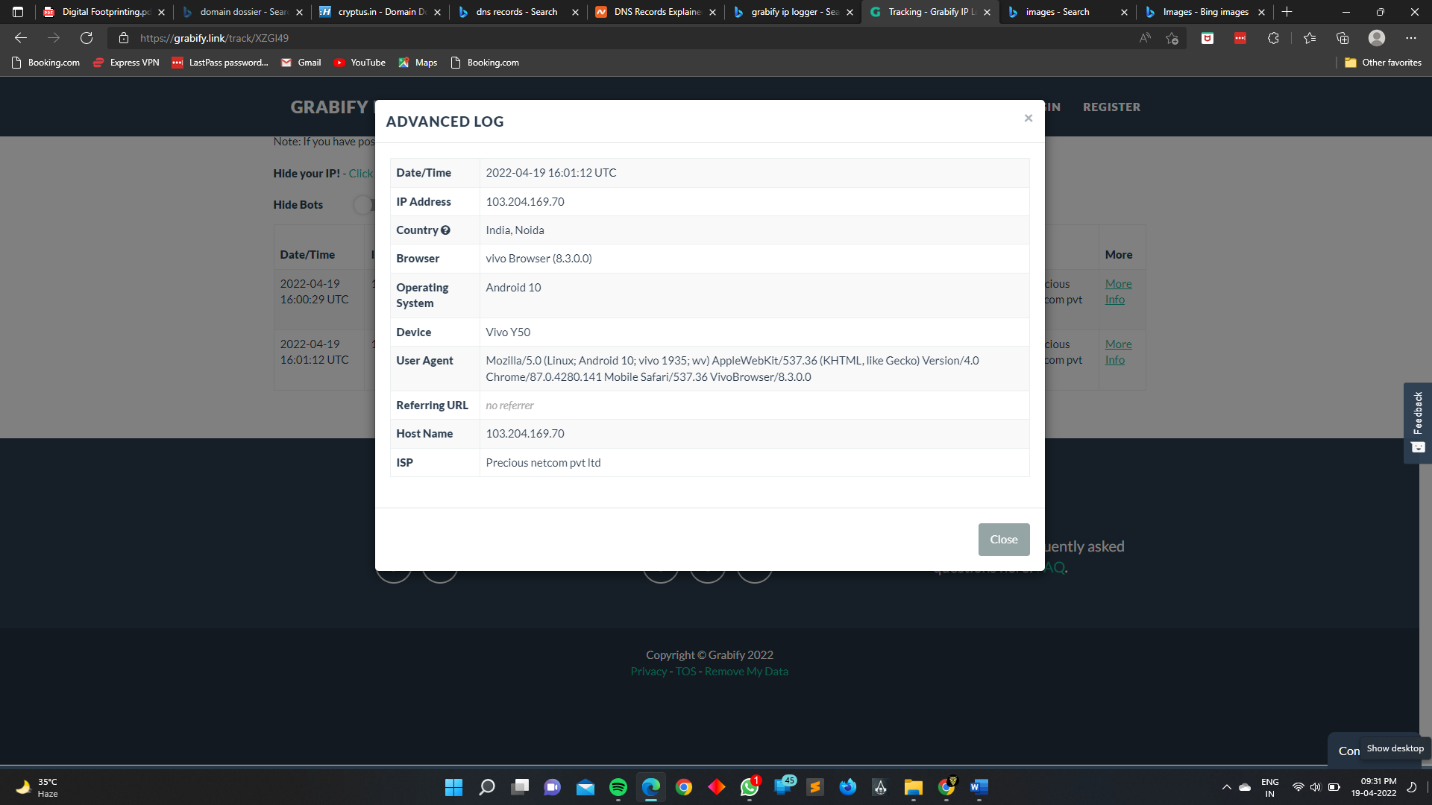
Website :- [cryptus.in - Domain Dossier - owner and registrar information, whois and DNS records (centralops.net)](https://centralops.net/co/domaindossier.aspx)

GRABIFY IP LOGGER



Website :- <https://grabify.link/>

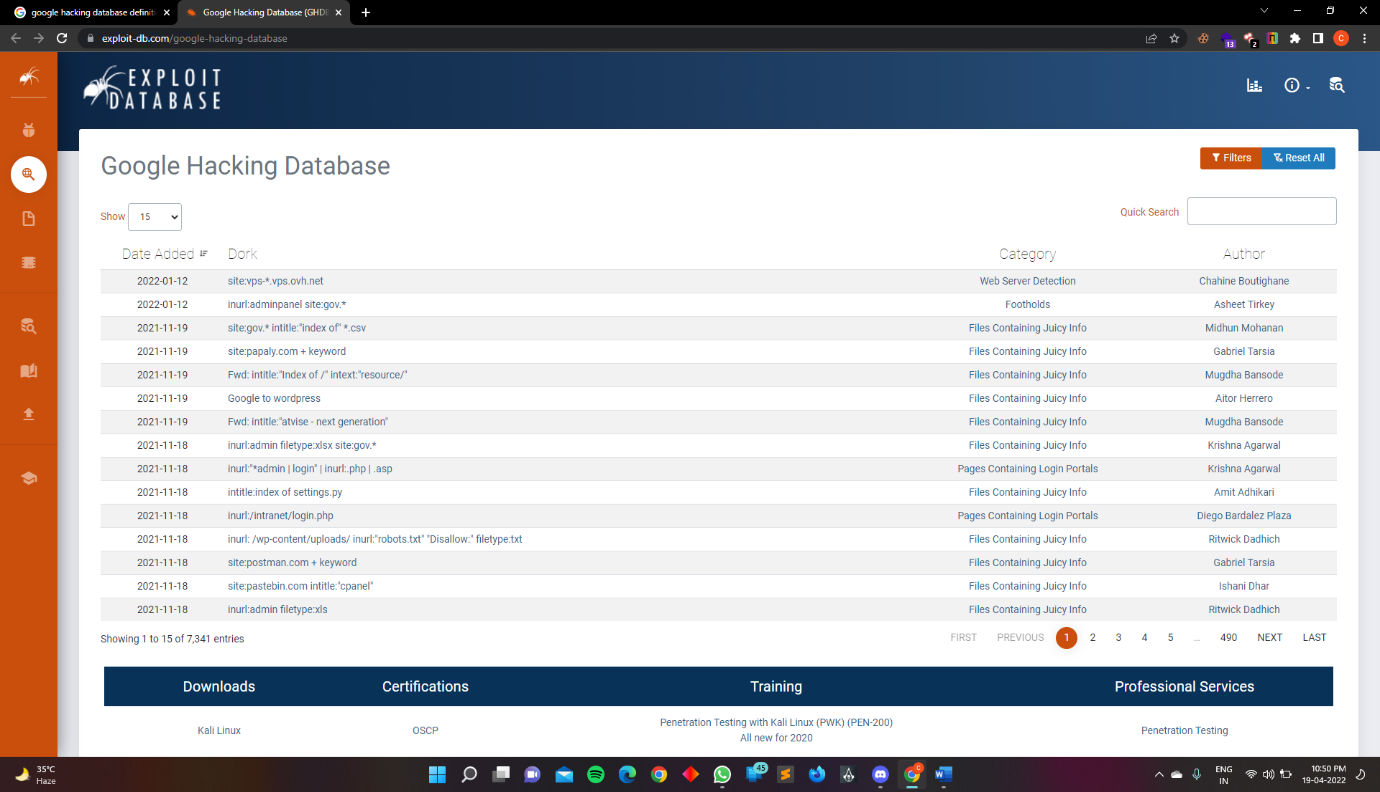




With the help of this tool we get the information about the target public Ip address, Android Version , country name , Host Name, ISP , Device name.. etc …

Google Hacking Database

The Google Hacking Database (GHDB) is **a compendium of Google hacking search terms that have been found to reveal sensitive data exposed by vulnerable servers and web applications**. The GHDB was launched in 2000 by Johnny Long to serve penetration testers.



Thank You