**Foot Printing**

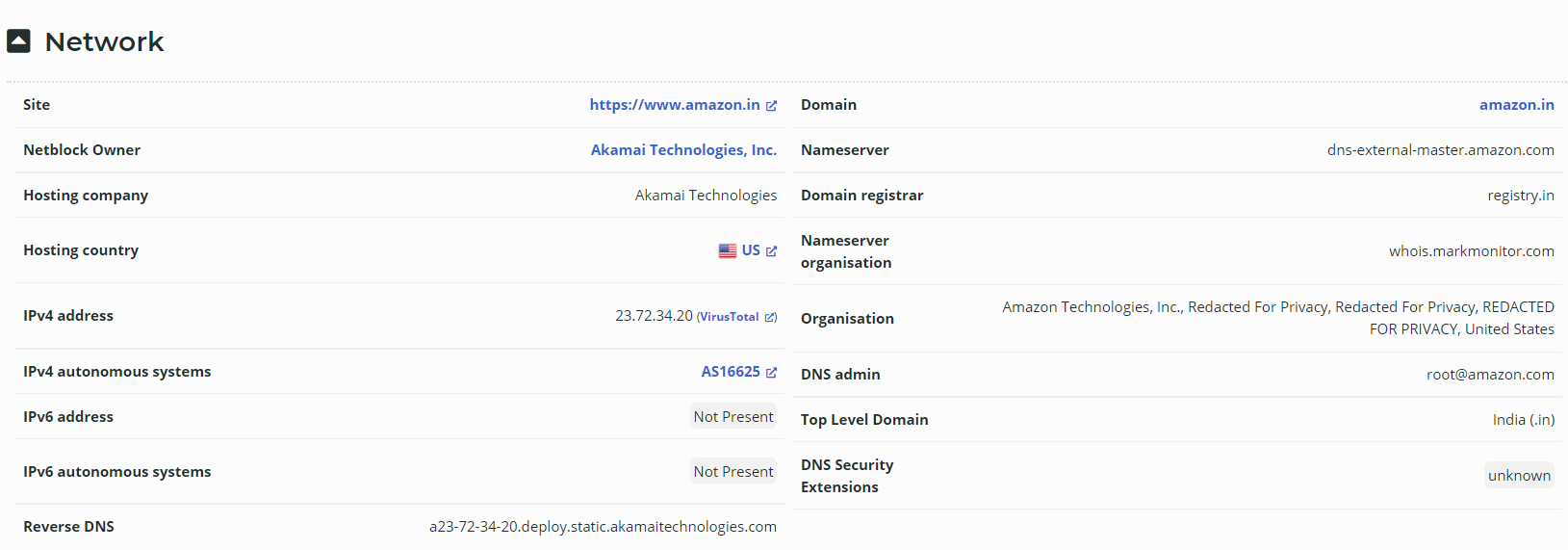
**Tools Used: NetCraft, Whois Domain System,Shodan,DnsDumpster**

**Target Site:** [www.amazon.in](http://www.amazon.in)

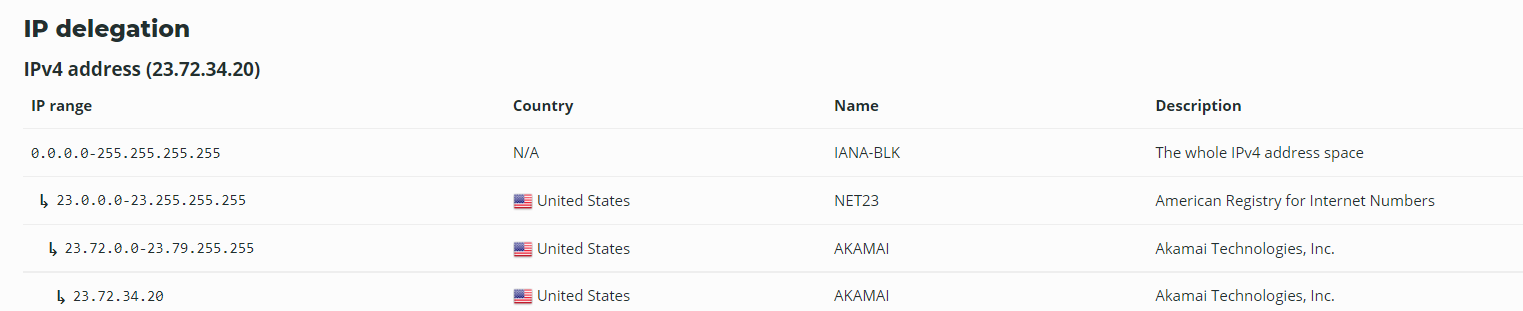
**Info Gathered using NetCraft**

**1)So first set of information we get is about the network, we can see the various information regarding amazon.in and which will be vital to gain access , or make the company believe that you are legit**

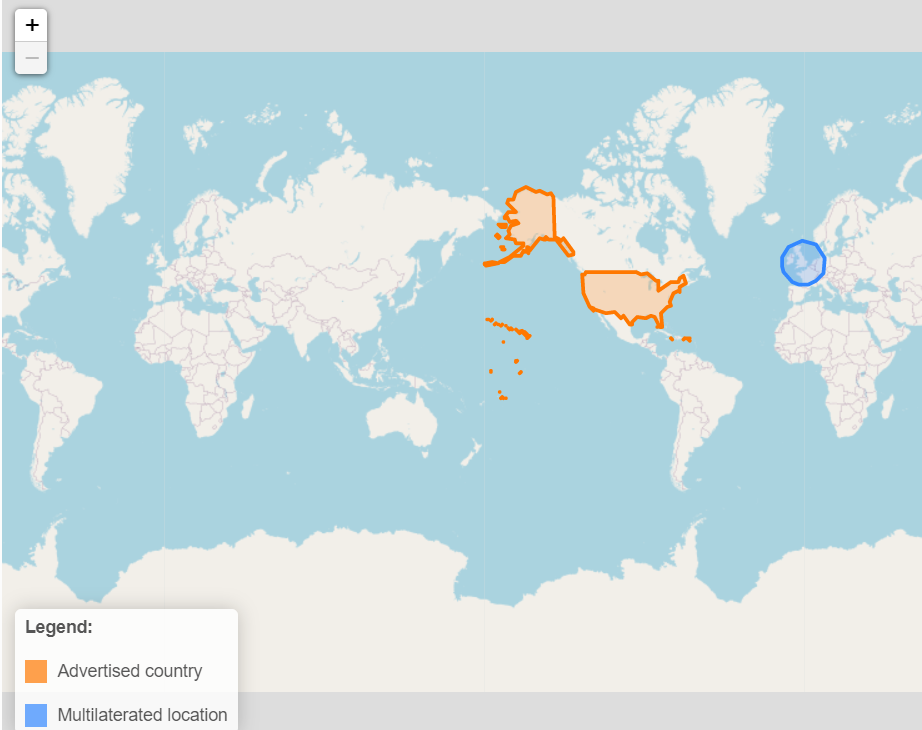
**Eg: hosting company, ip addr, etc**



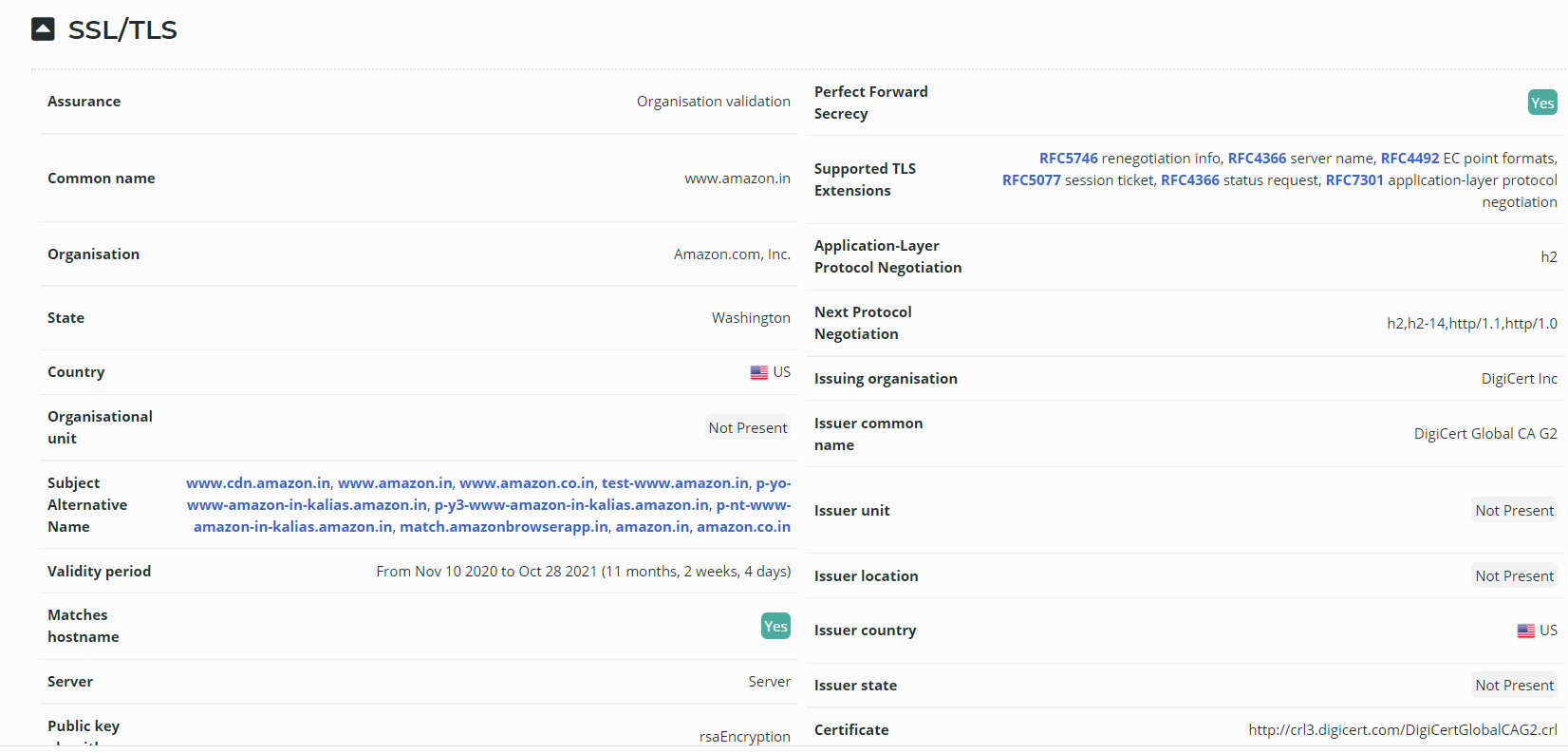
**This shows the various Ip addr that are associated with the company**



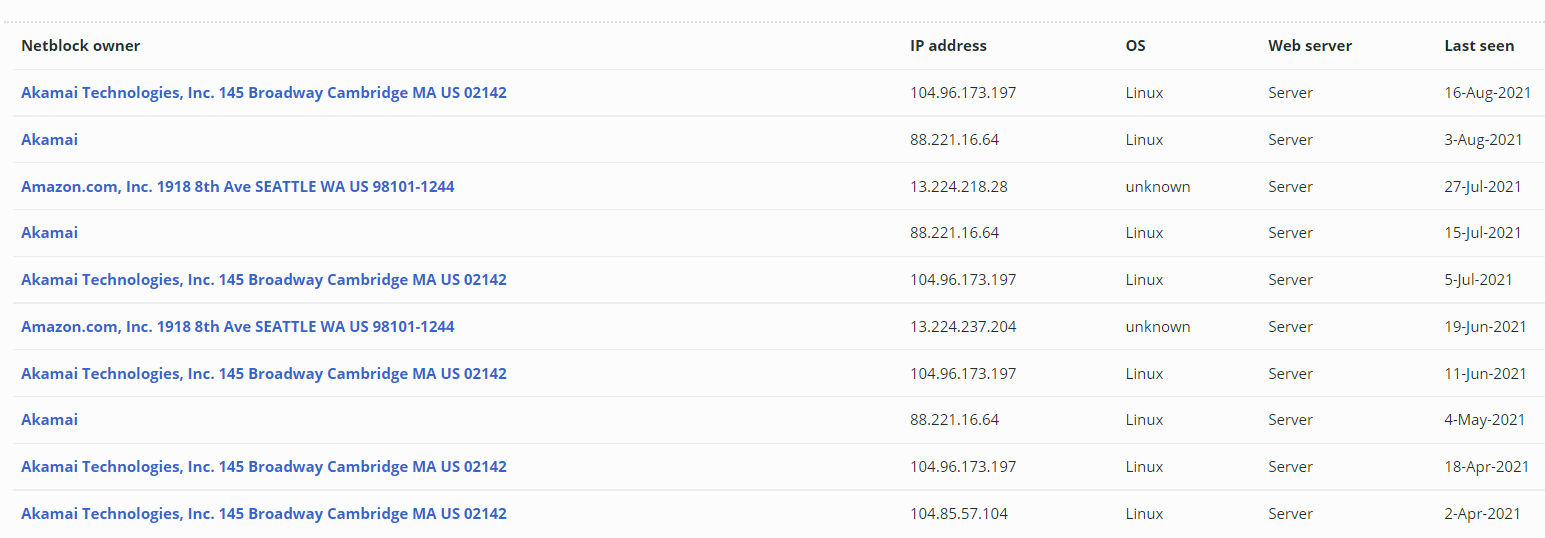
**Possible Server Location**



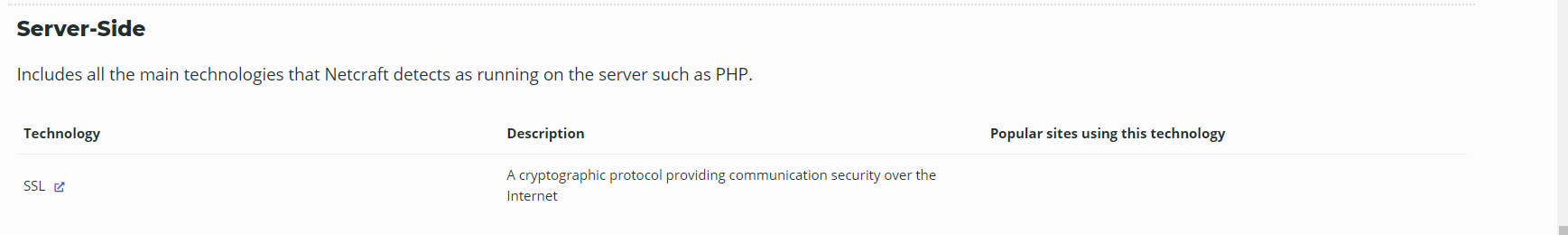
**SSL Certification details**

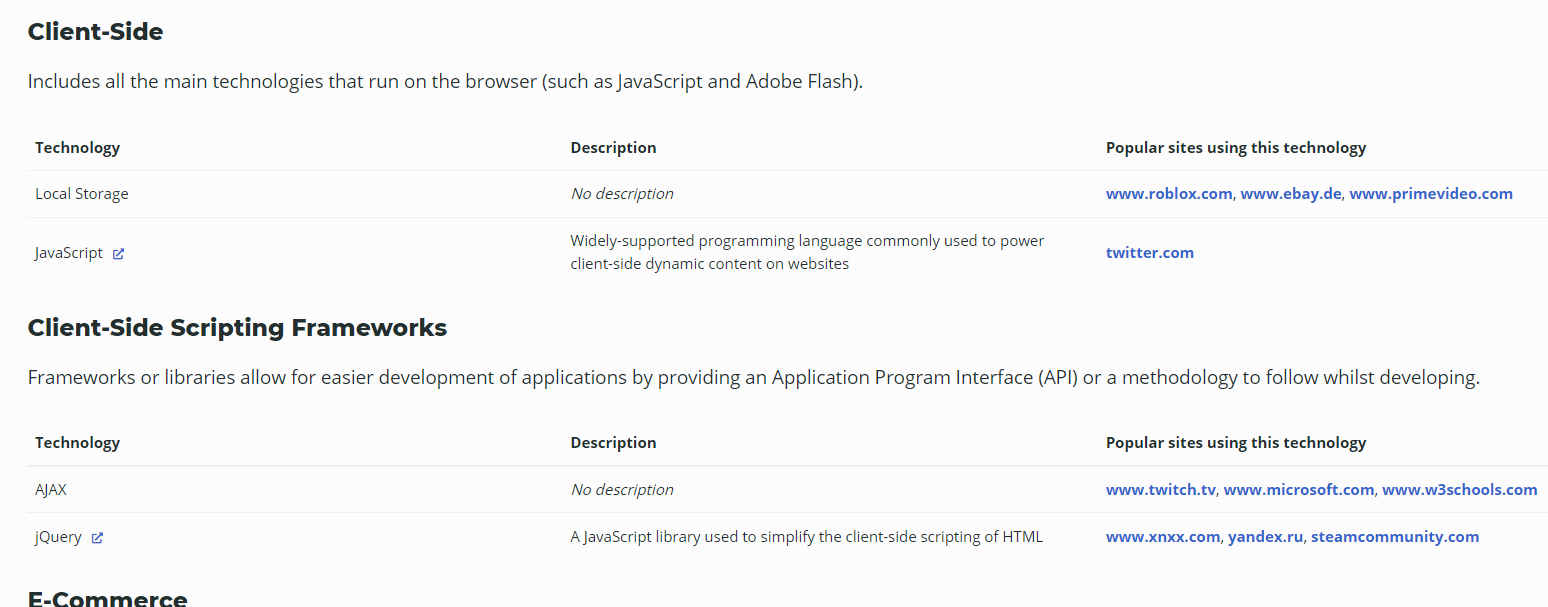


**Server Hosting History**



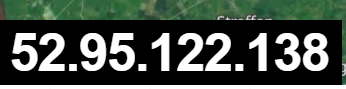
**Client and Server side technologies and frameworks**

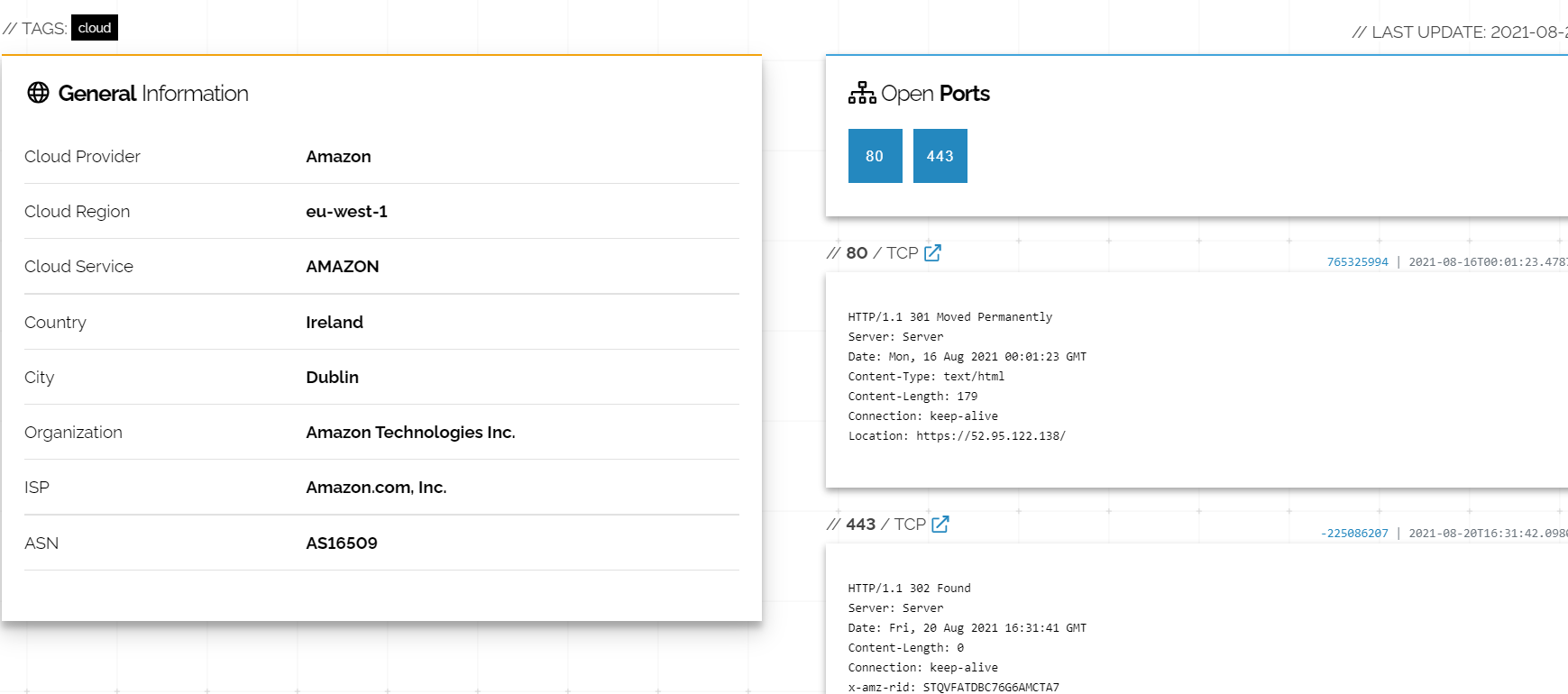




**Shodan is another great online platform that lets us know what all types of systems,webcams , routers are being implemented**

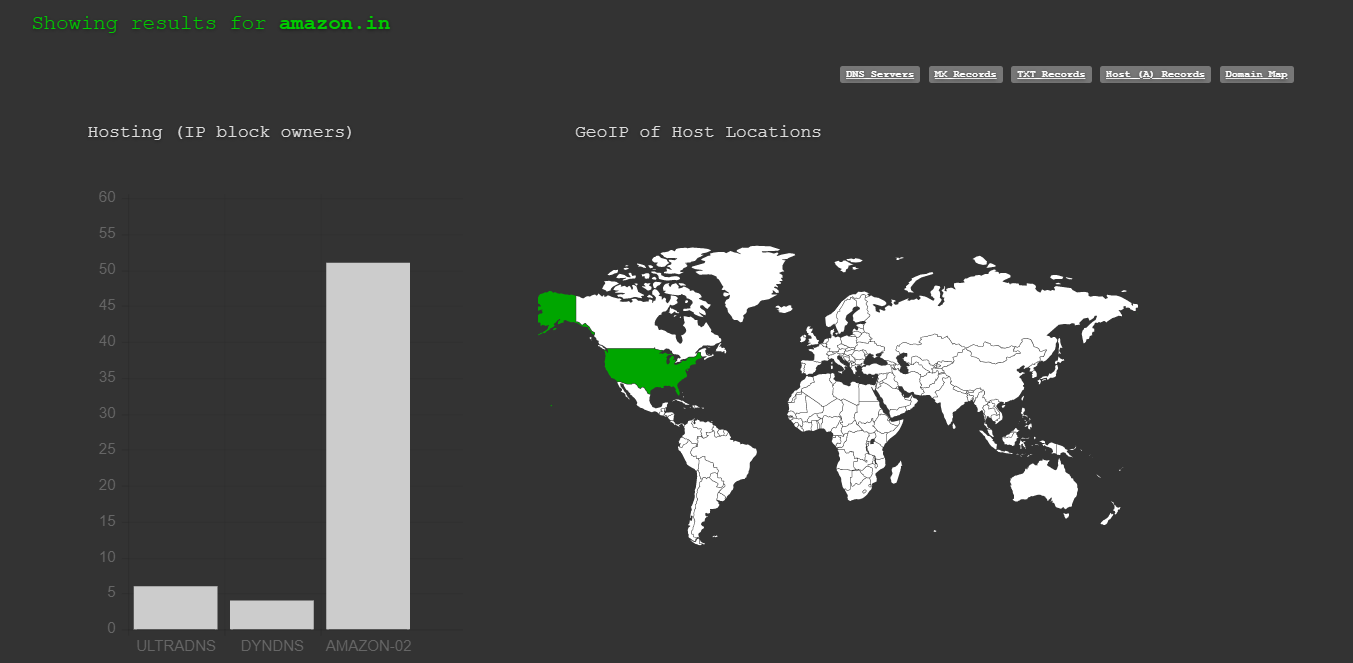
**For example : here I have certain valuable information regarding a cloud server used by amazon present in Ireland, not only I am able to get the ports available to me but all also the ip addr the ssl certificate and so much more**

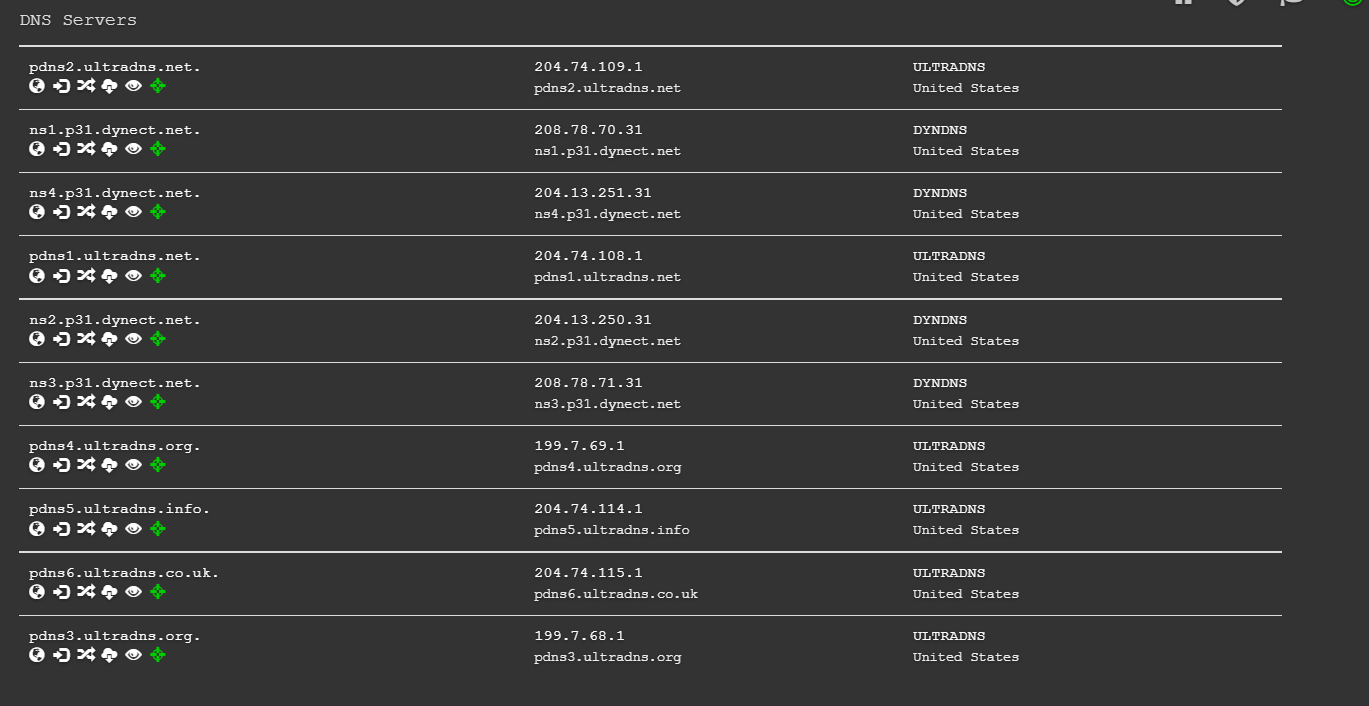




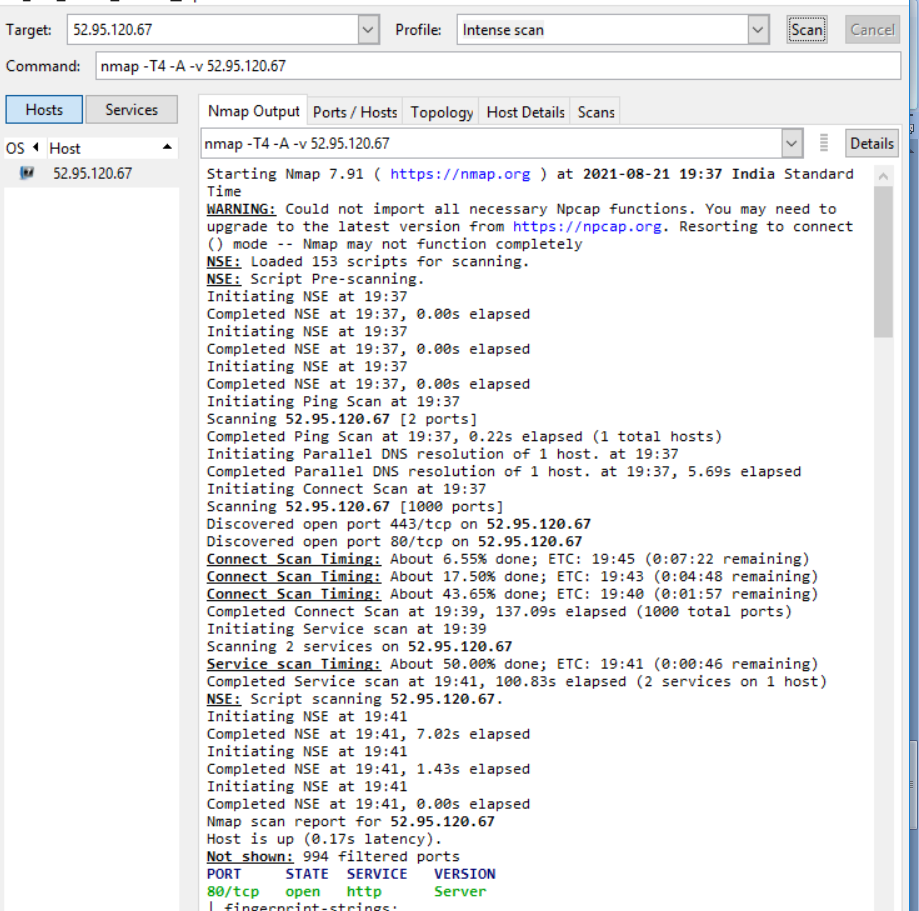
**Next I gathered Information regarding the Domains used by the target site with the help of dns dumpster**

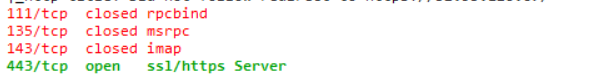
**Here I was able to gather all the domains used by amazon**





**Another Major Tool for footprinting is nmap tool and also the nmap command in kali linux of any given ip address**





**In Kali linux, nmap can also provide information regarding the routers,webcams and so on.**