INVESTIGATING IP ADDRESSES CAPTURED BY WIRESHARK DURING NETWORK ANALYSIS

BY

SOMKENE RICHARD

26th OCTOBER,2024

EXECUTIVE SUMMARY

The IP addresses within the network traffic for the domains **blockchainunn.org** and **app.ether.fi** were analyzed using specified tools. During this analysis, one IP address along the network route was identified as malicious by VirusTotal, posing a serious concern for network communication. Some common IPs were found after the domain captures, indicating that the two domains shared a common network pathway in which one of them happened to be a private IP . Remediation steps were also provided to address the potential vulnerability arising from the malicious IP discovered.

INTRODUCTION

IP addresses are sets of numbers assigned to computers for communication over a network or the Internet. Domain names also have designated IP addresses that facilitate communication between a client and a server. When a client sends a packet to a server or domain over a network, it passes through several intermediate IPs or networks, a process which can be observed using a tool called traceroute, before reaching its destination

TOOLS

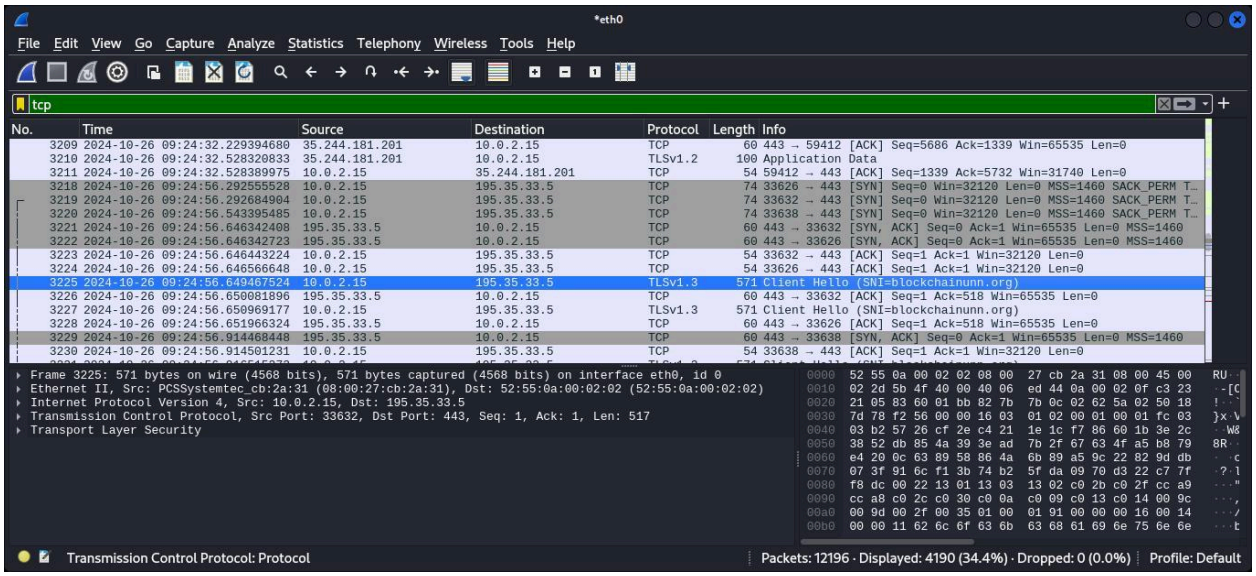
Whoer.net

Virustotal

Abuseipdb

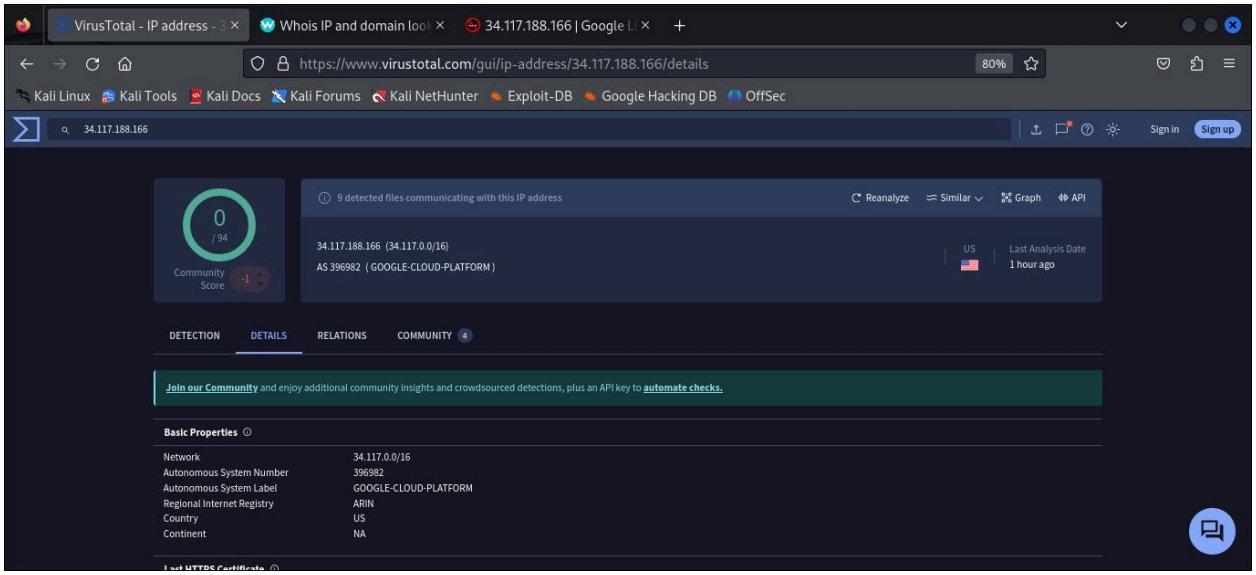
ANALYSIS

A. For blockchainunn.org

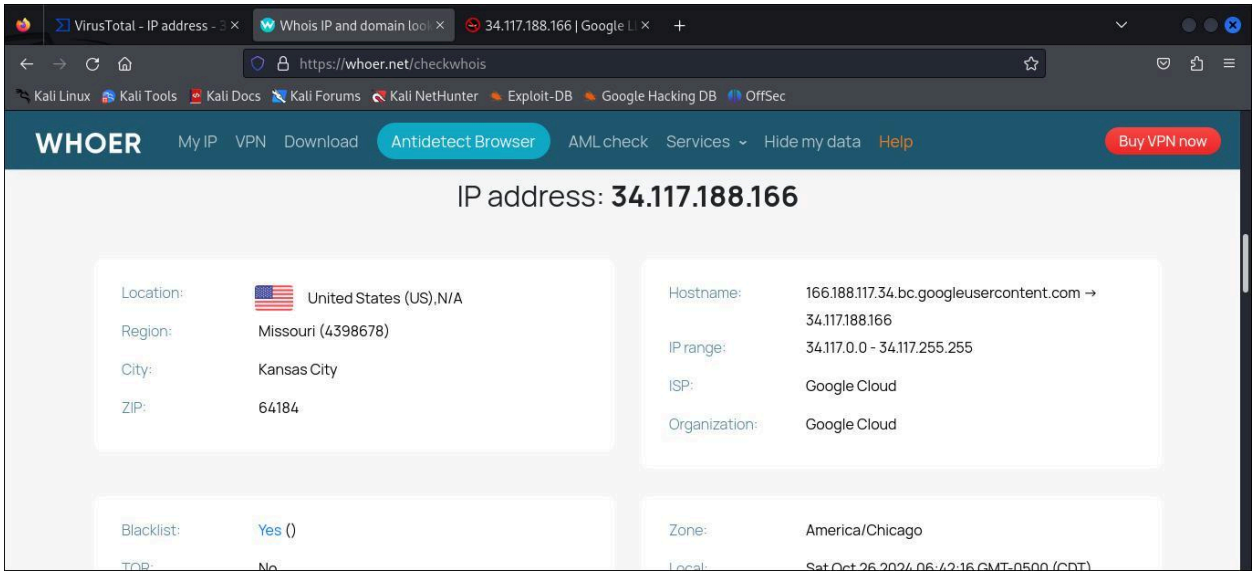


An overview of the packet details captured on Wireshark during the access to blockchainunn.org domain

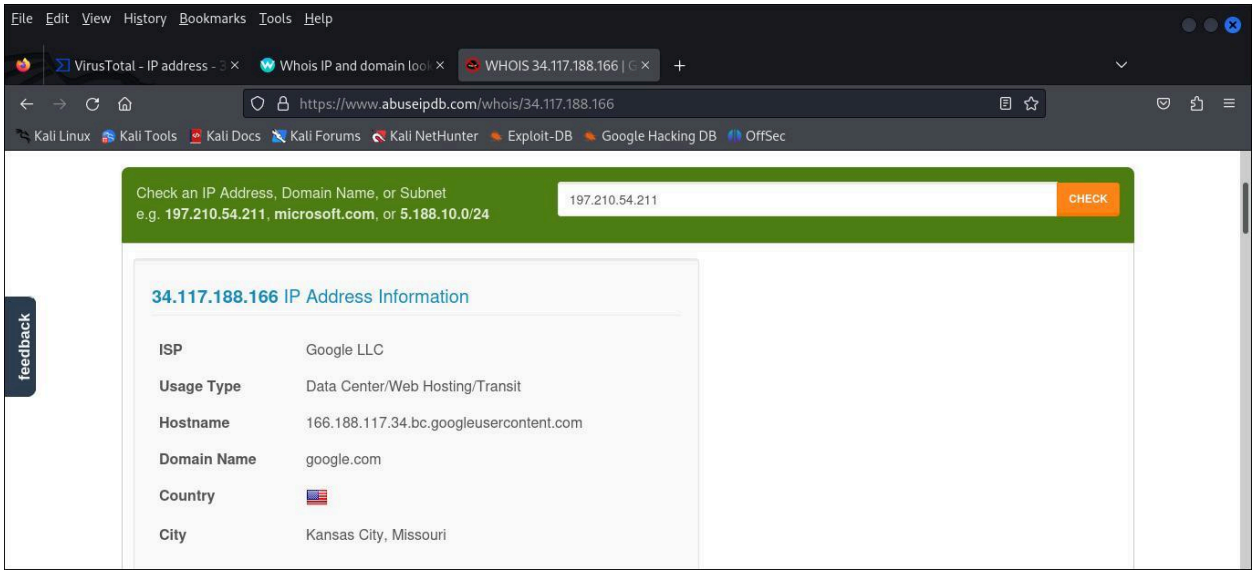
IP address 34.177.188.166



Scan result on virustotal showing this IP belongs to Google cloud

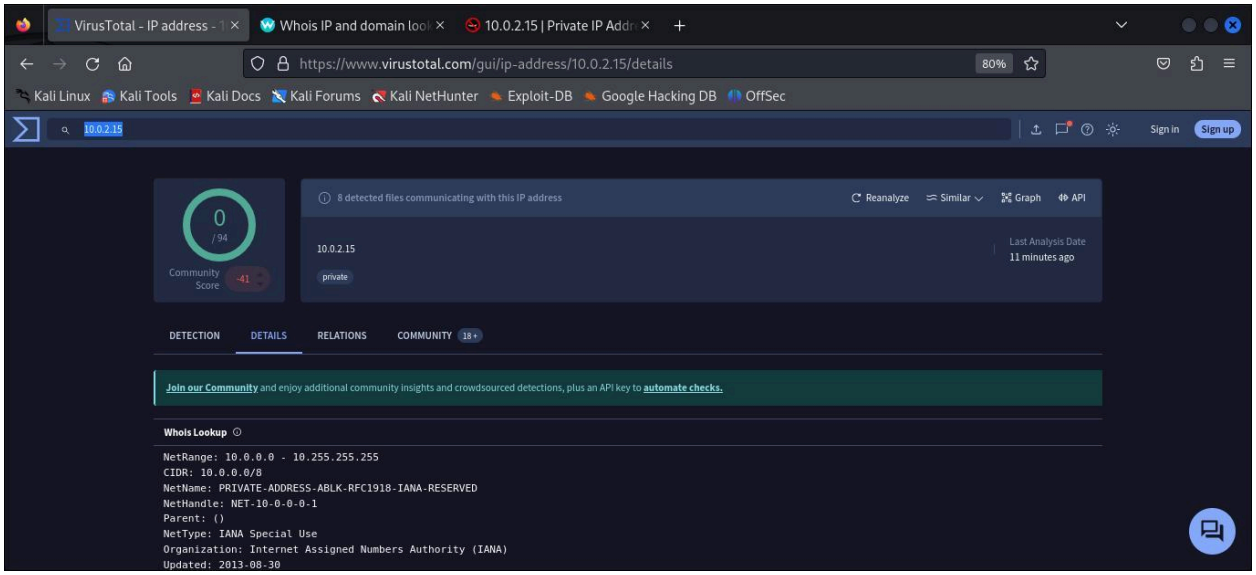


Scan result on whoer.net

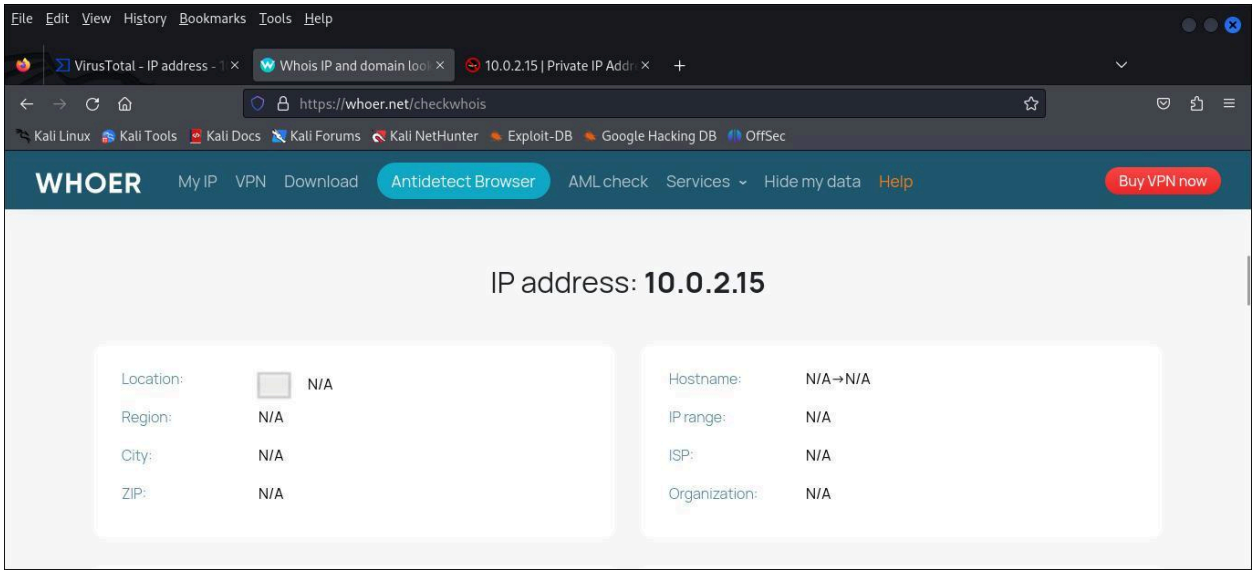


Scan result on abuseipdb

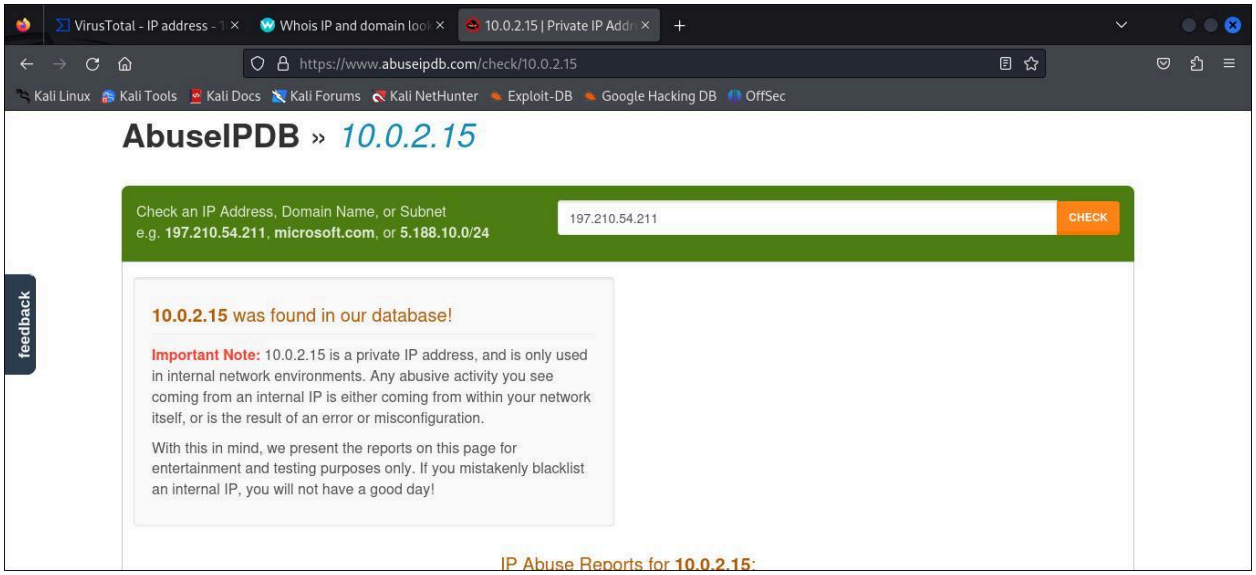
IP address 10.0.2.15



Scan result on virustotal showing this IP address is a private IP

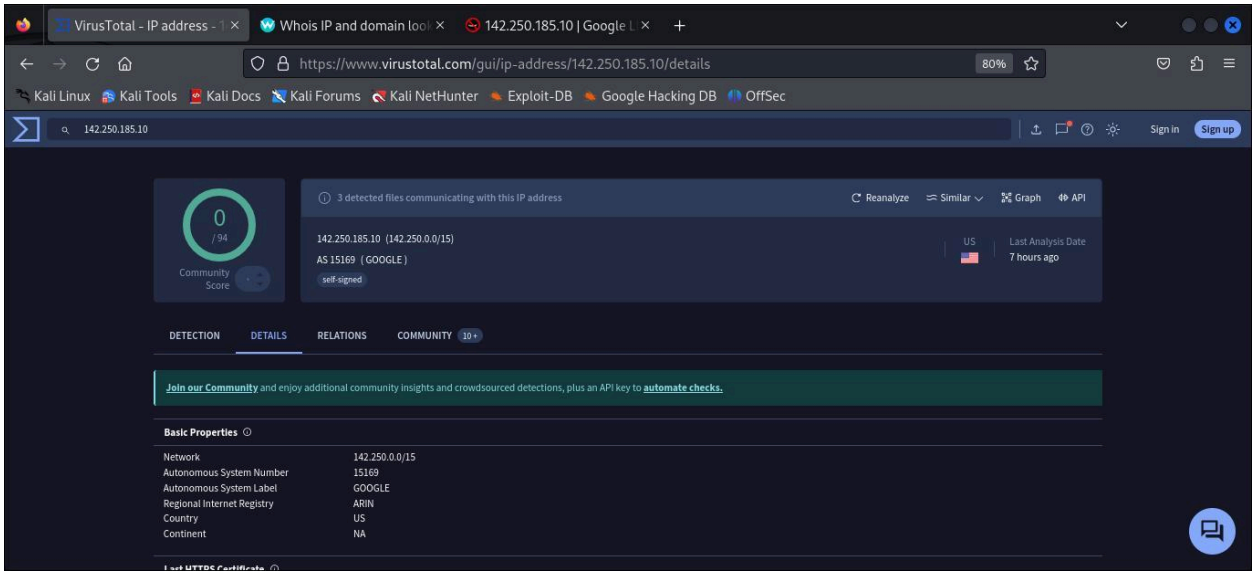


Scan result on whoer.net

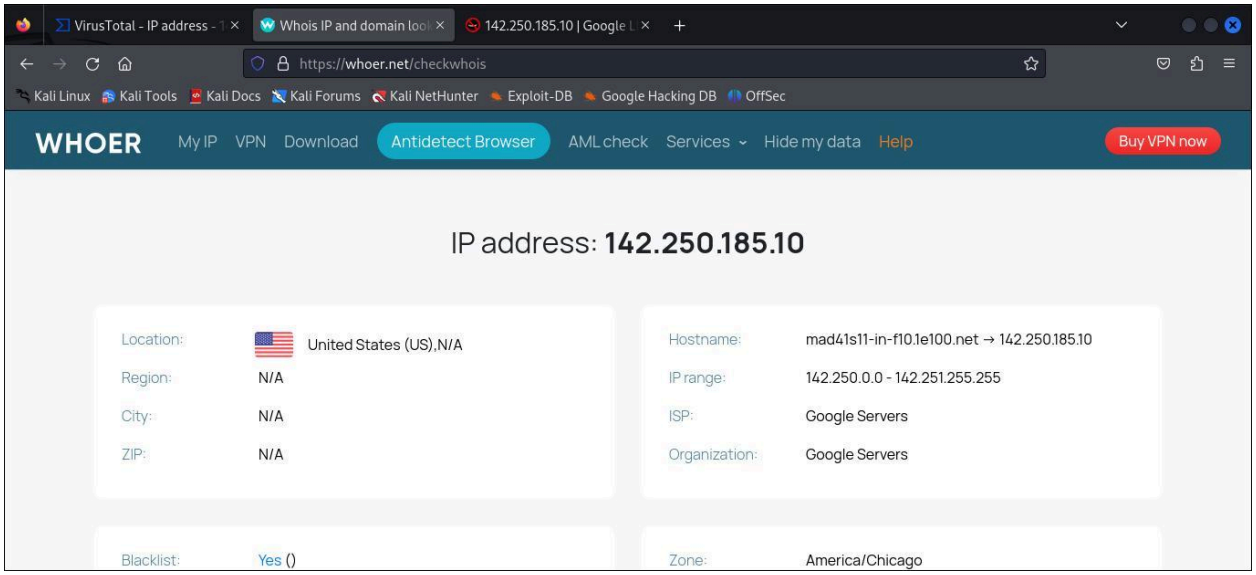


Scan result on abuseipdb

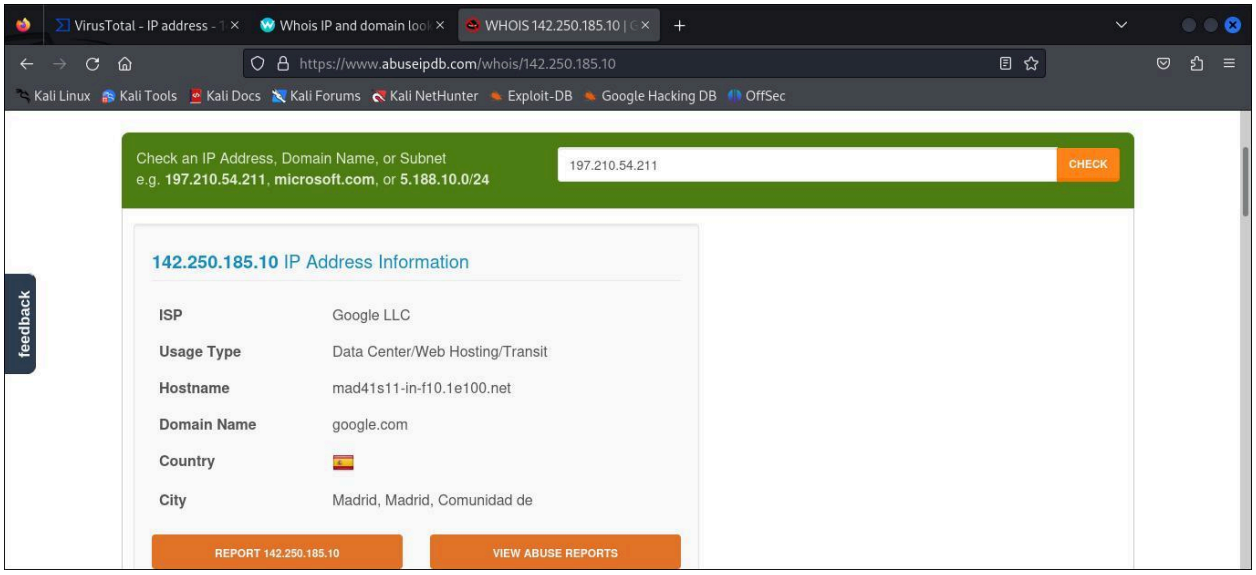
IP address 142.250.185.10



Scan result on virustotal showing that this IP belongs to Google and is self-assigned as well

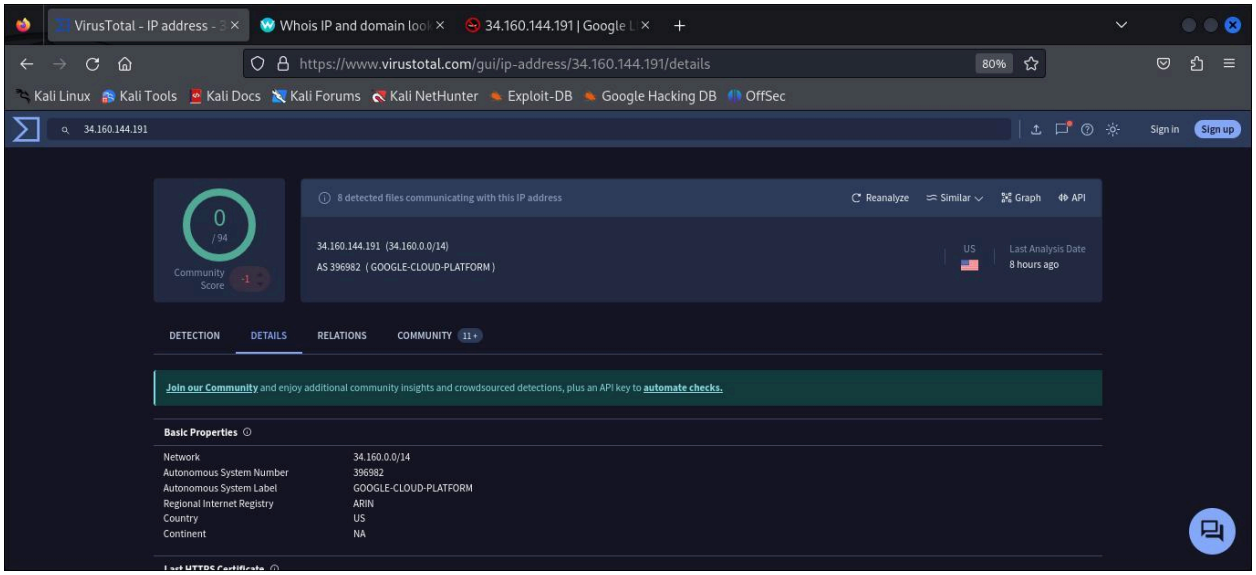


Scan result on whoer.net

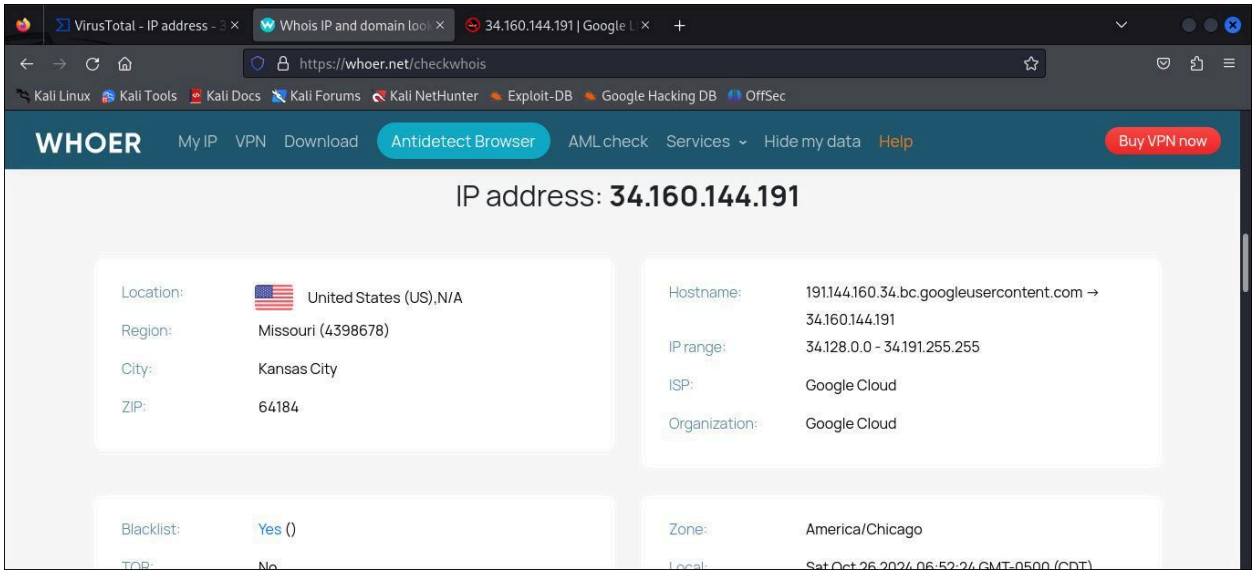


Scan result on abuseipdb

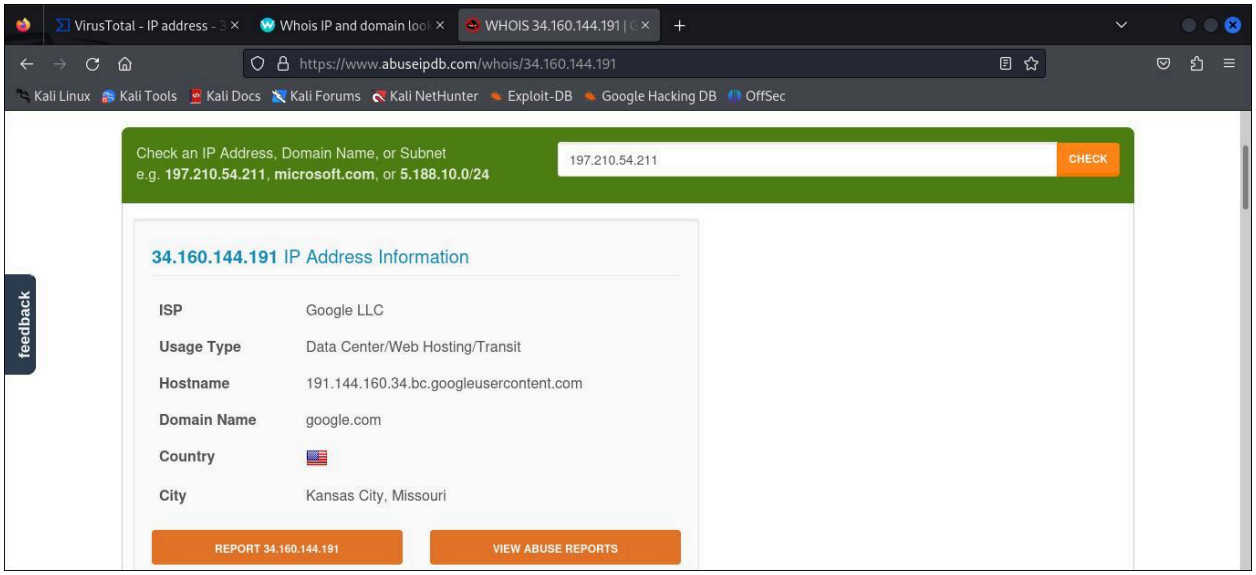
IP address 34.160.144.191



Scan result on virustotal showing this IP belongs to Google cloud

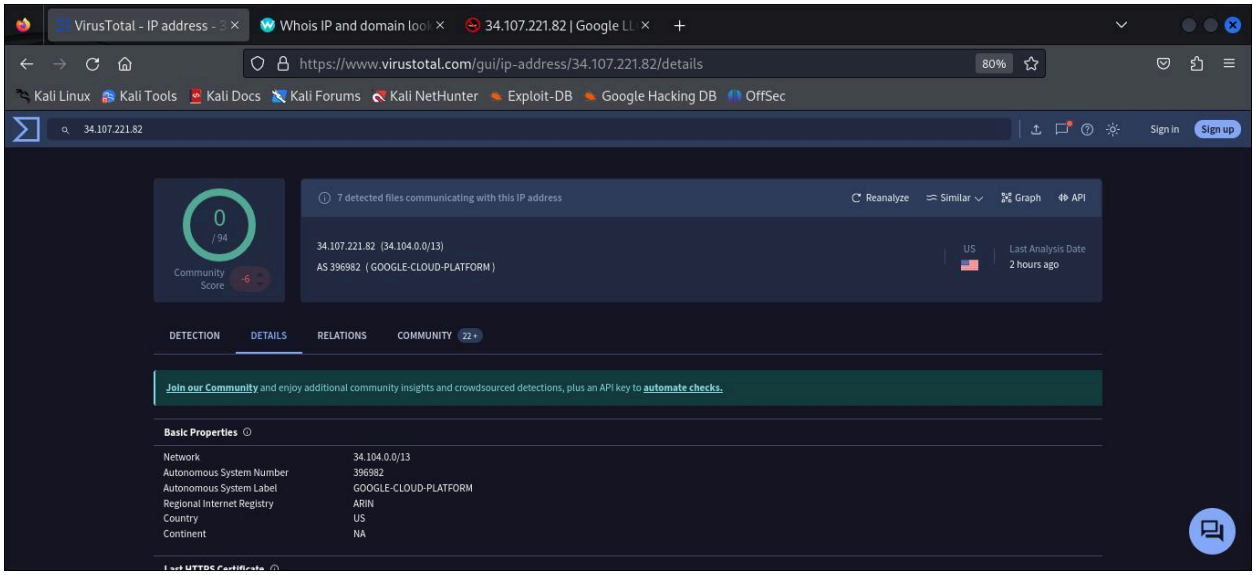


Scan result on whoer.net

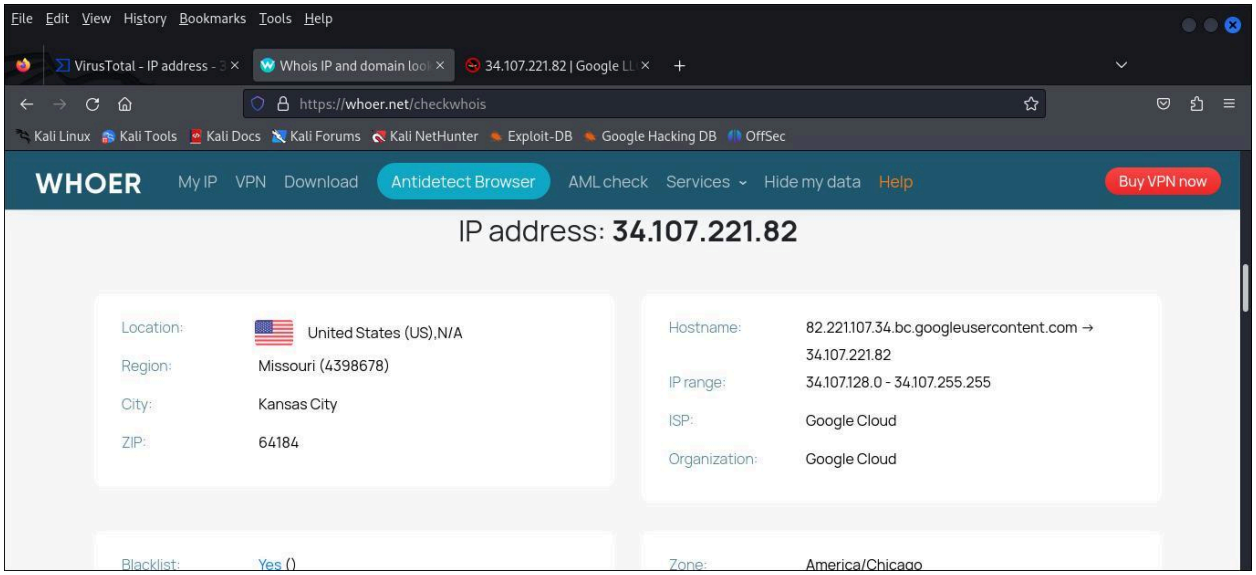


Scan result on abuseipdb

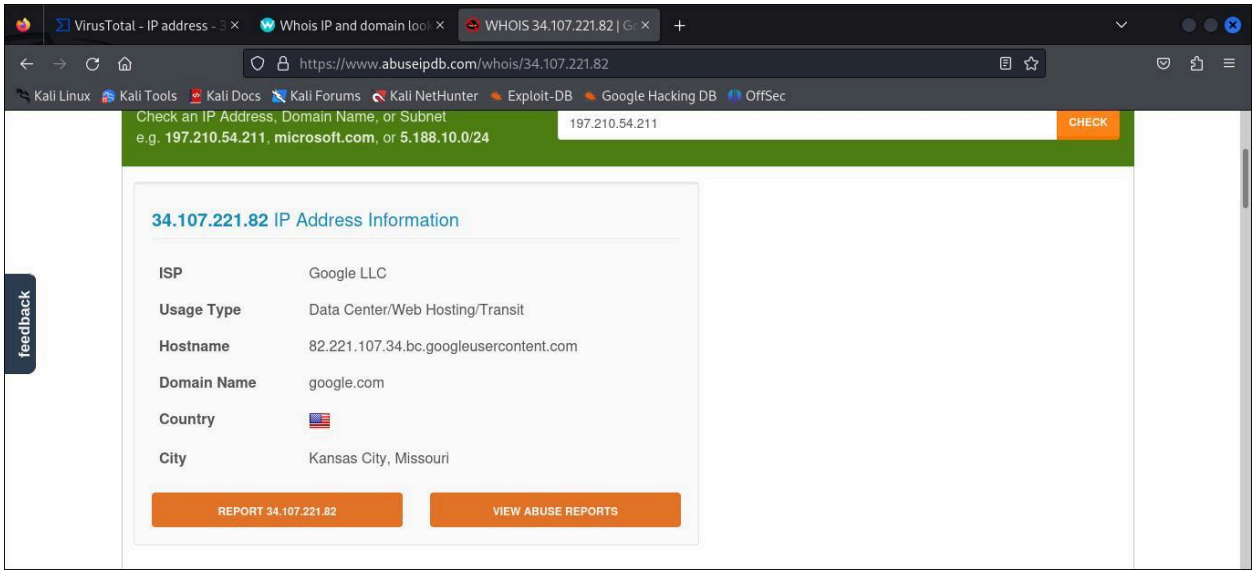
IP address 34.107.221.82



Scan result on virustotal showing this IP belongs to Google cloud

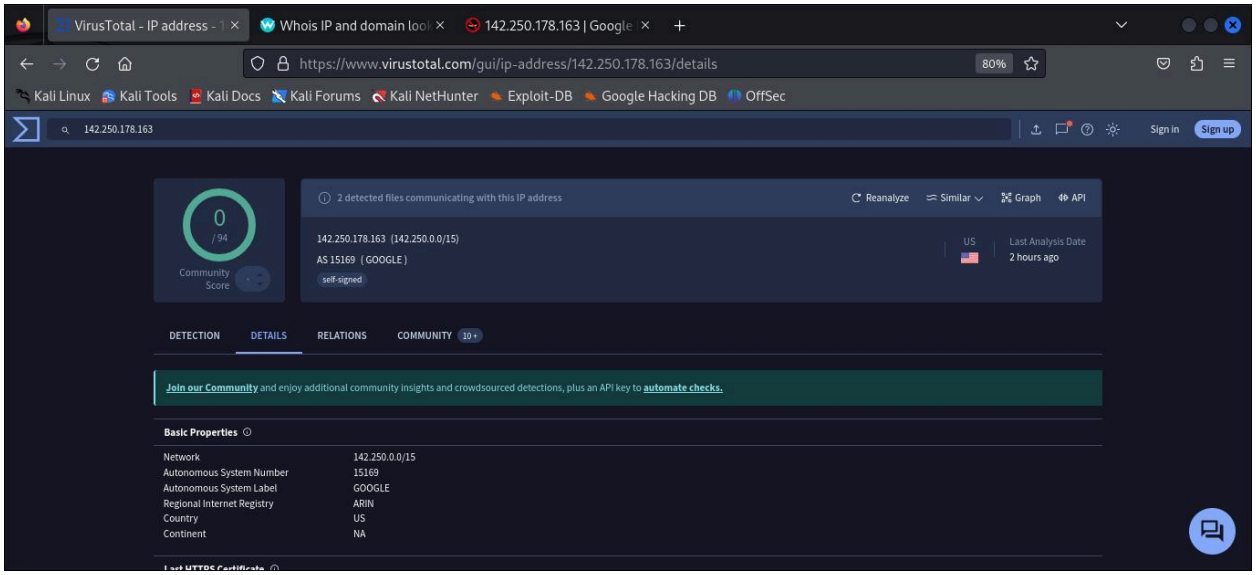


Scan result on whoer.net

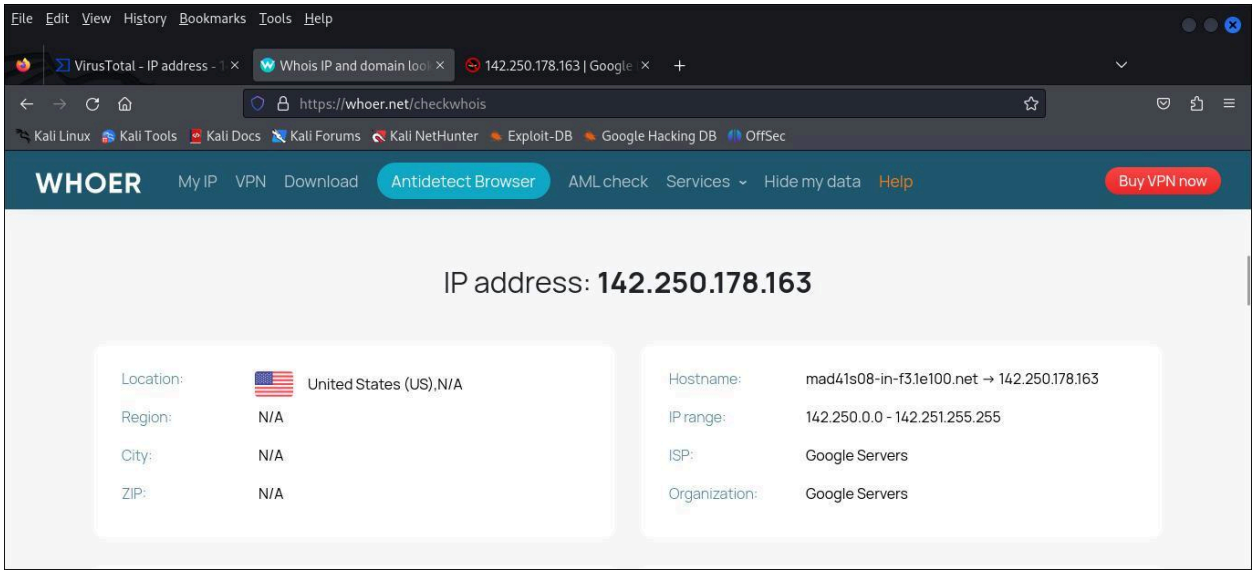


Scan result on abuseipdb

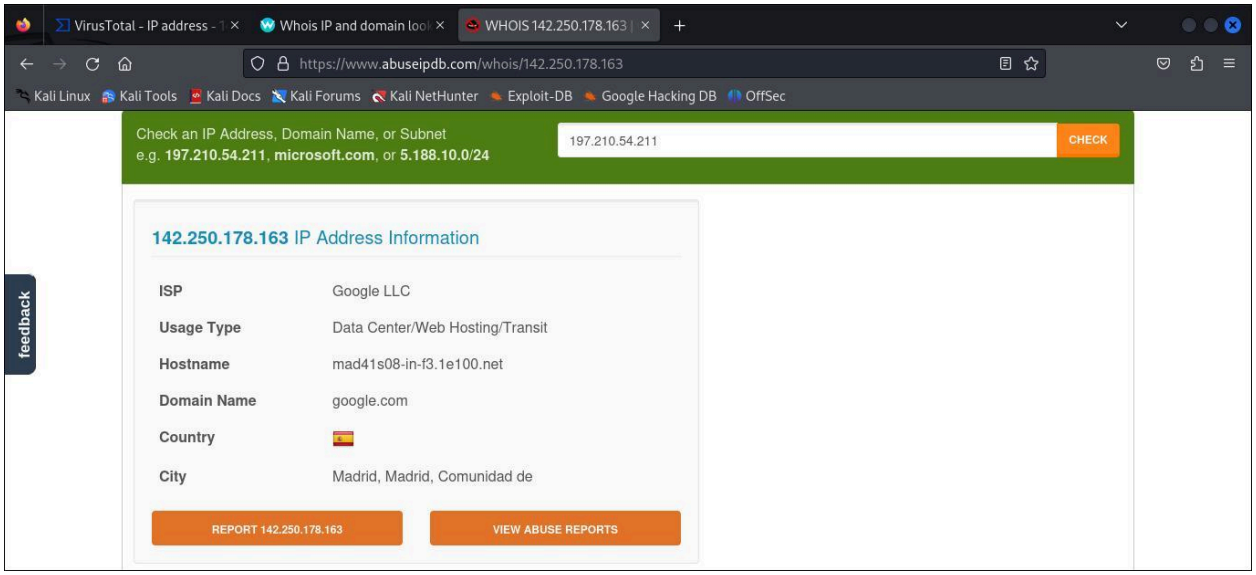
IP address 142.250.178.163



Scan result on virustotal showing this IP was self-assigned to Google

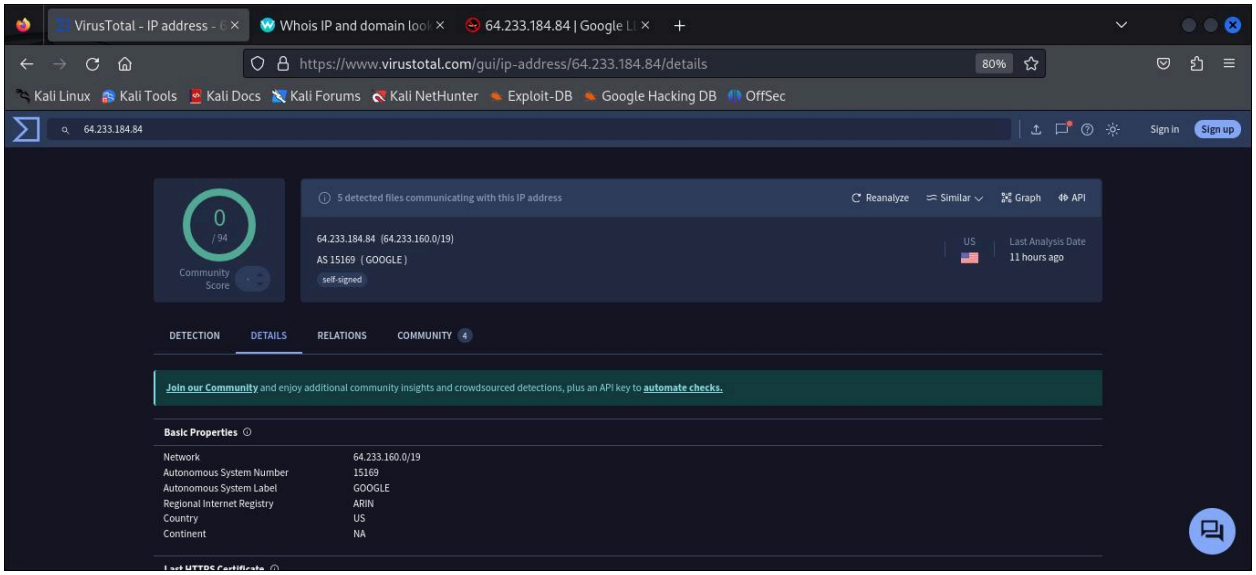


Scan result on whoer.net

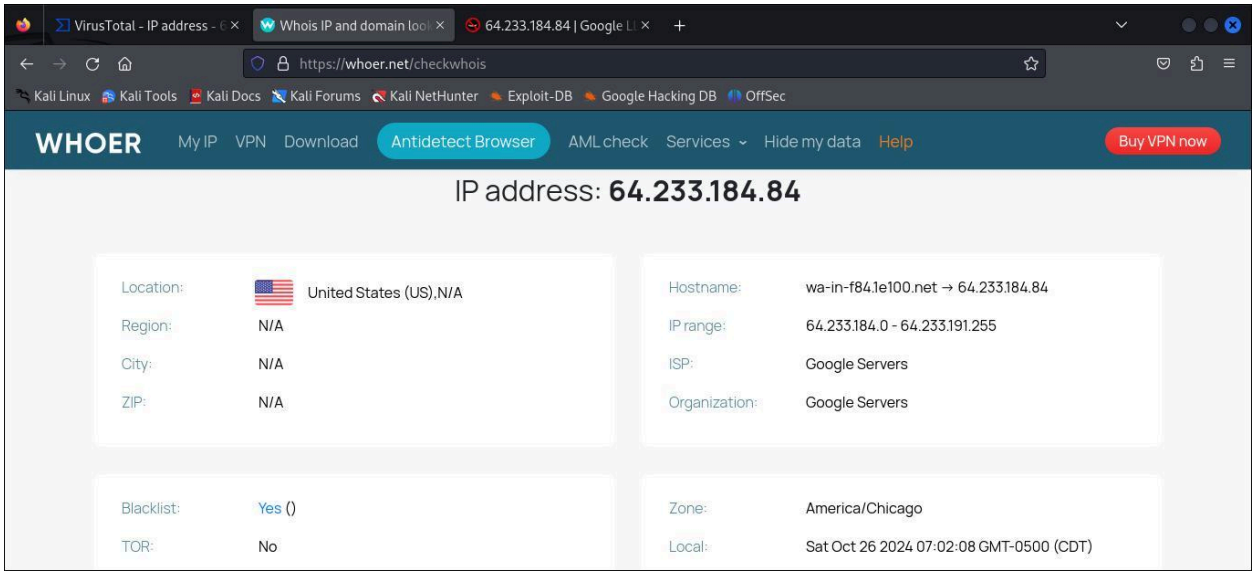


Scan result on abuseipdb

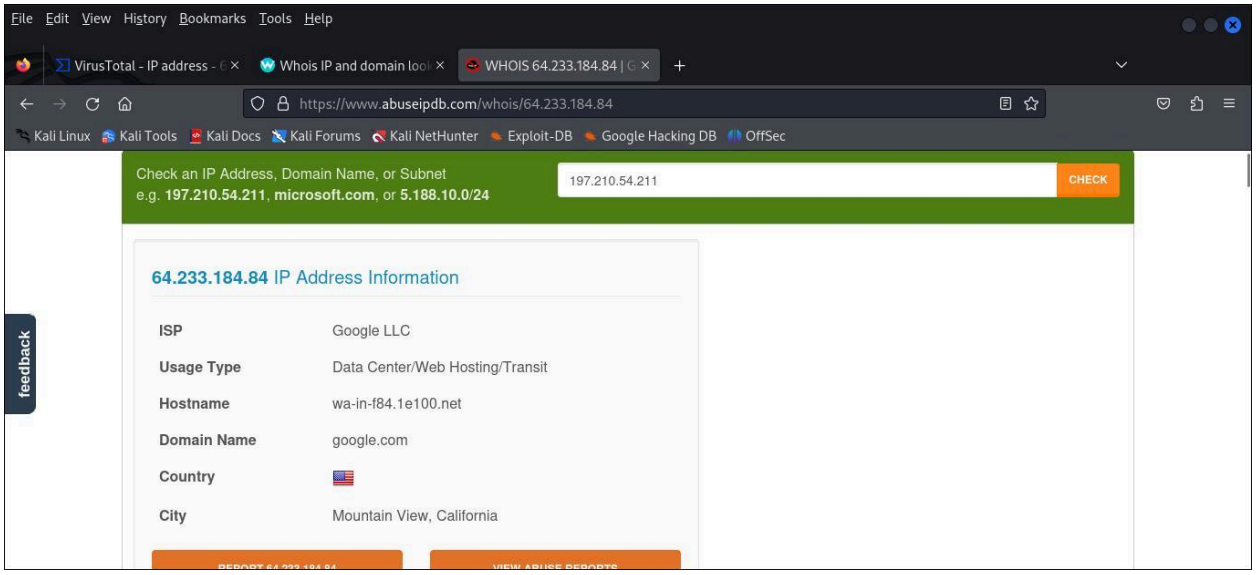
IP address 64.233.184.84



Scan result on virustotal showing this IP was self-assigned to Google

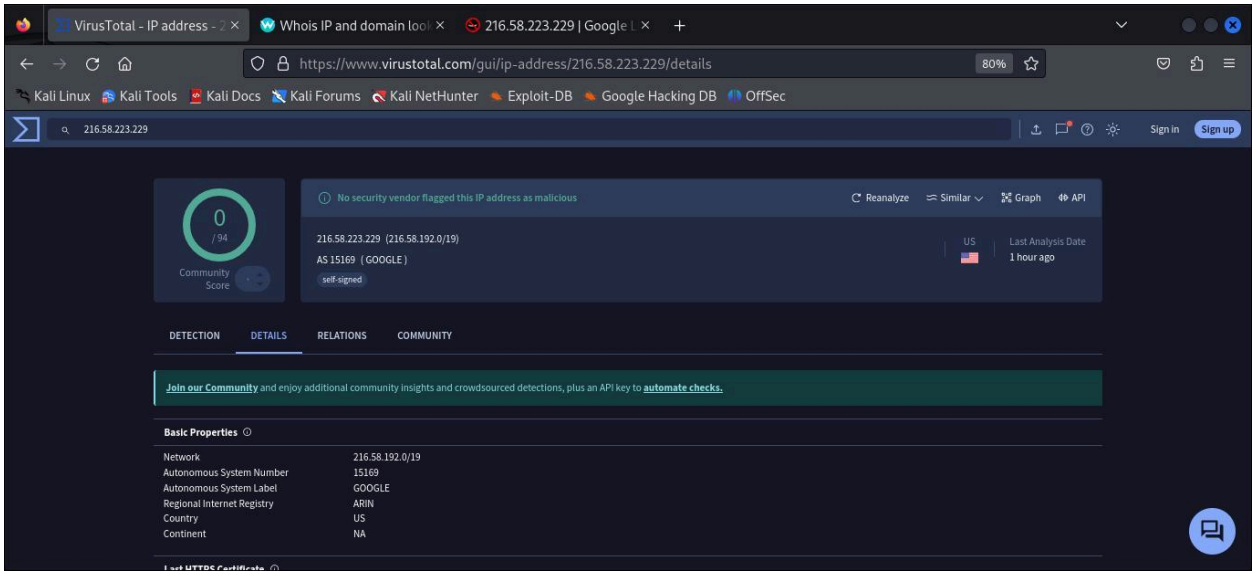


Scan result on whoer.net

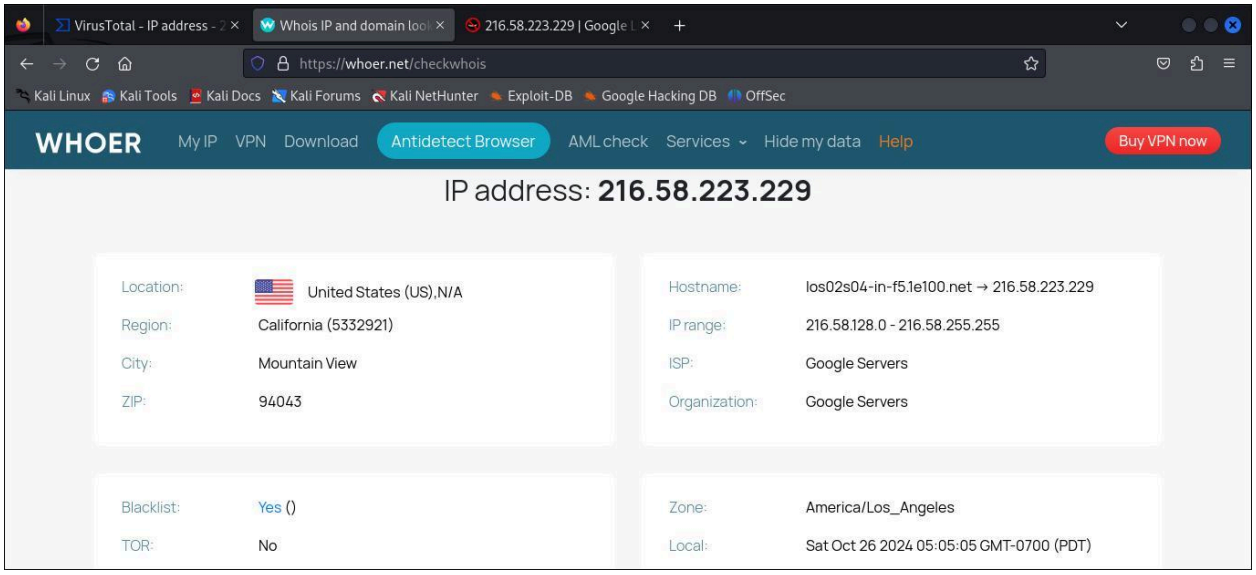


Scan result on abuseipdb

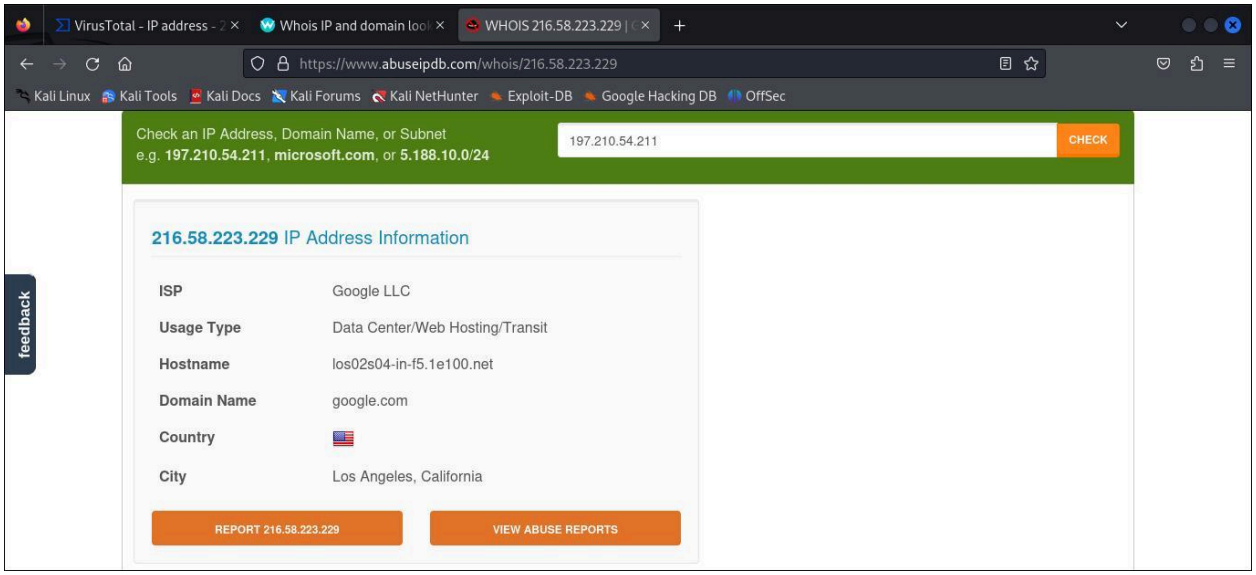
IP address 216.58.223.229



Scan result on virustotal showing this IP was self-assigned to Google

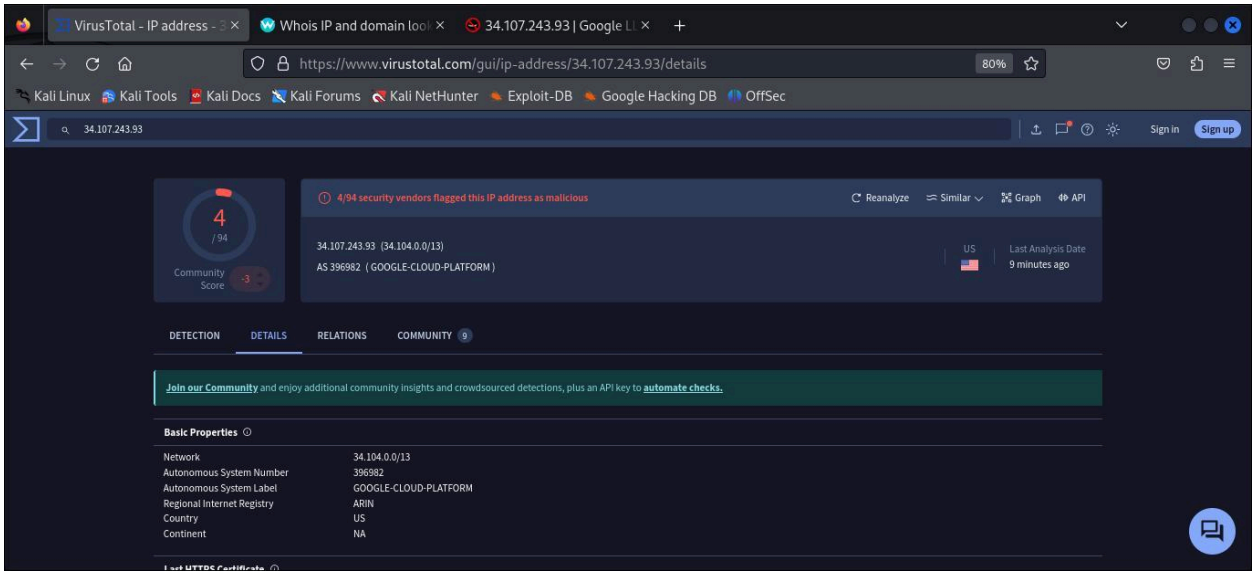


Scan result on whoer.net

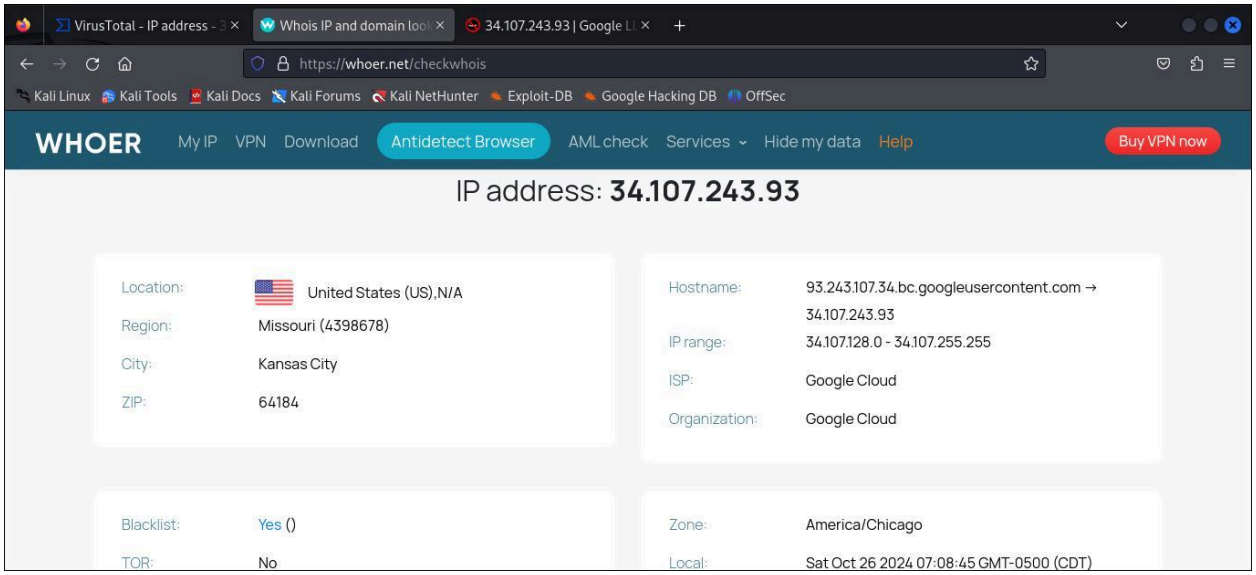


Scan result on abuseipdb

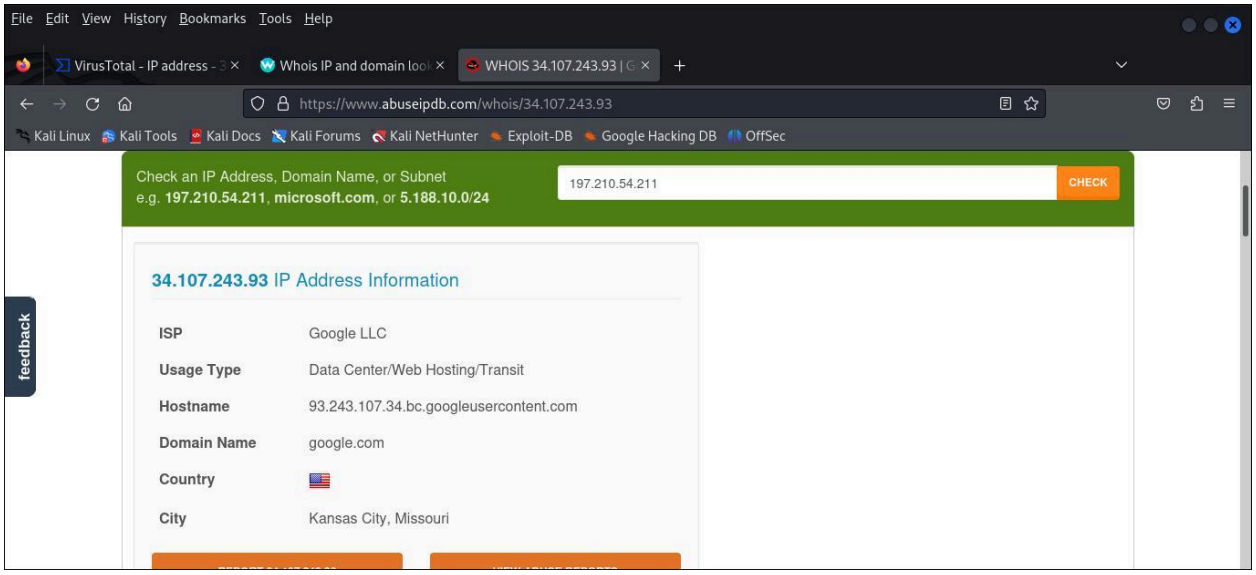
IP address 34.107.243.93



Scan result on virustotal flagging this IP malicious

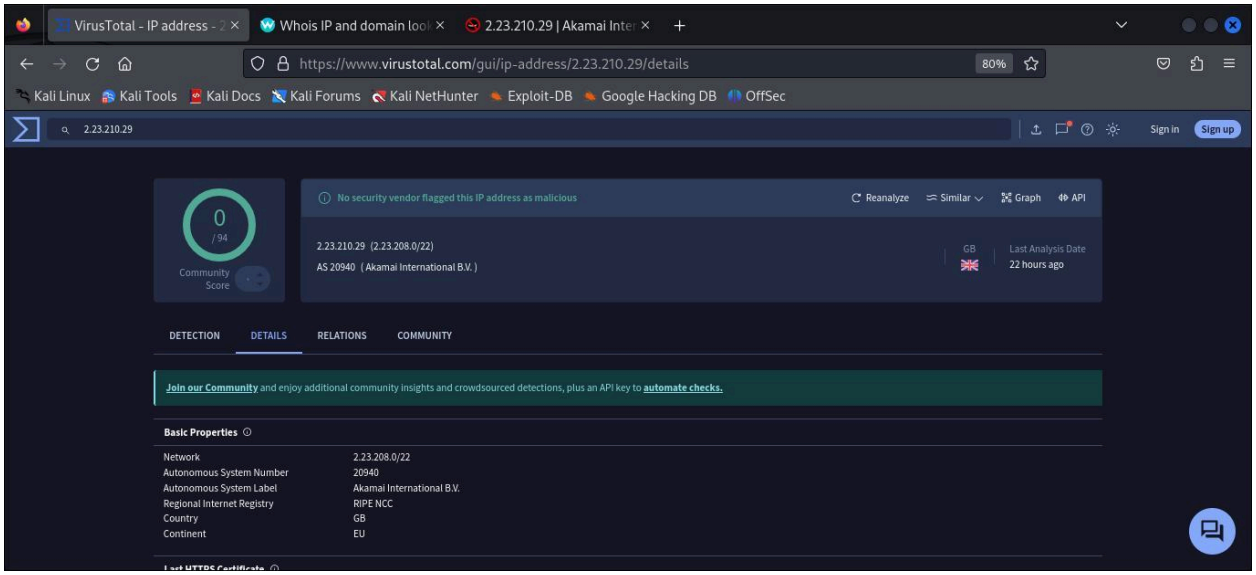


Scan result on whoer.net

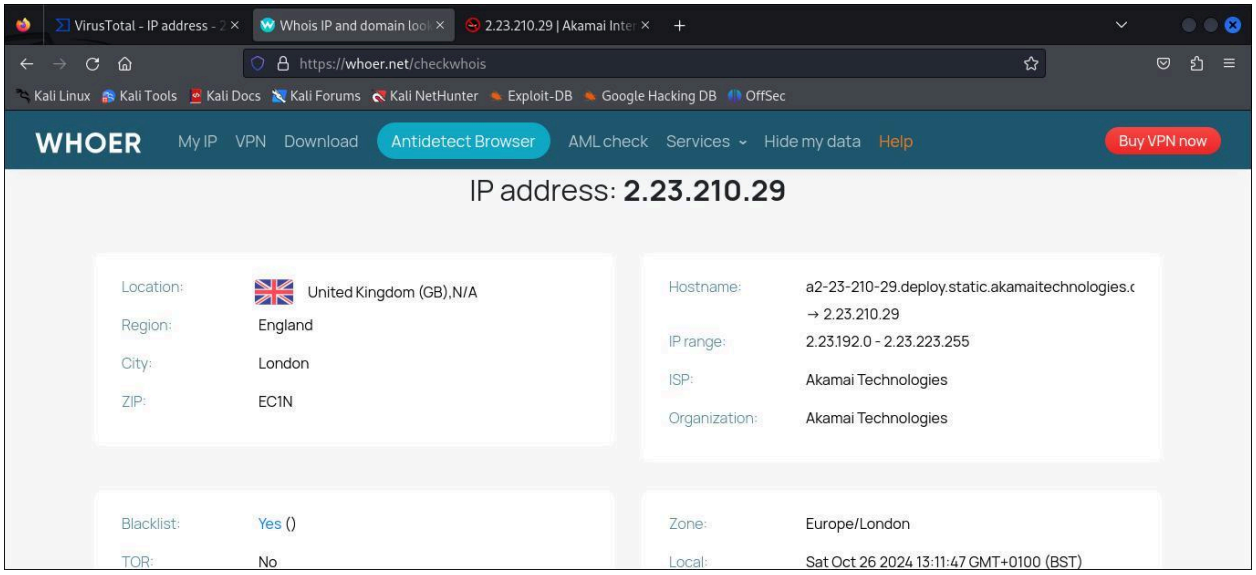


Scan result on abuseipdb

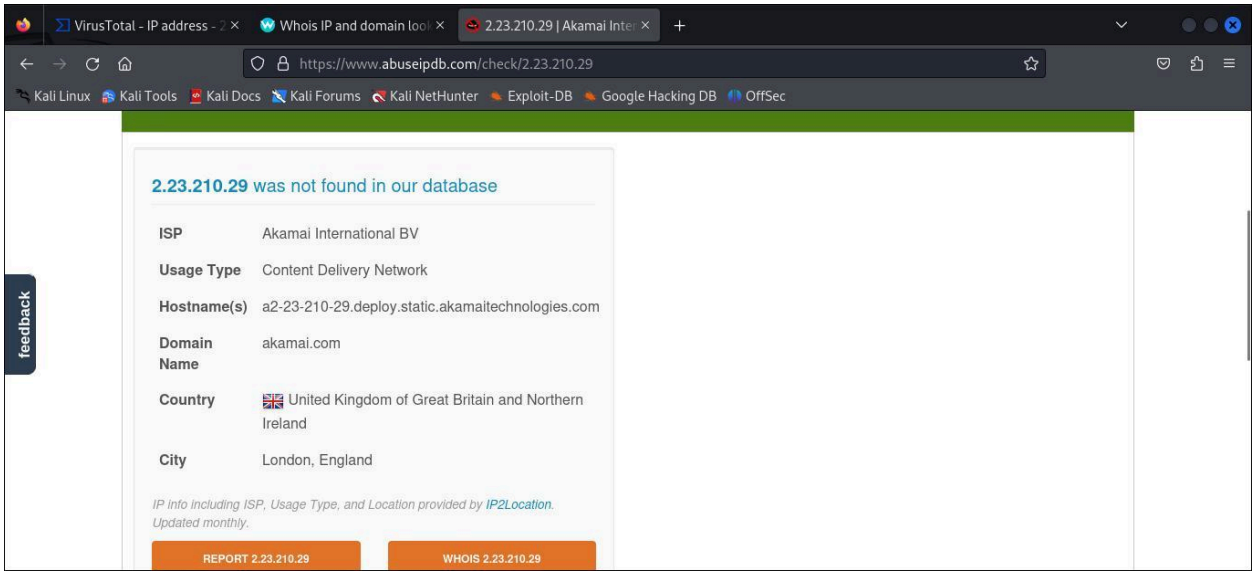
IP address 2.23.210.29



Scan result on virustotal showing this IP belongs to Akamal international B.V

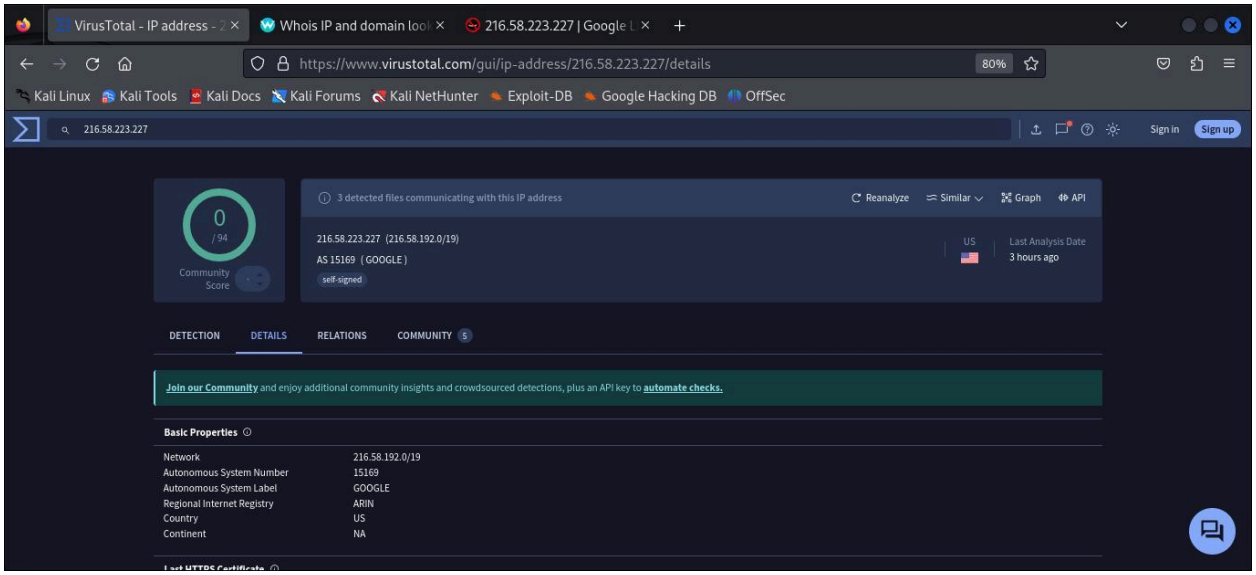


Scan result on whoer.net

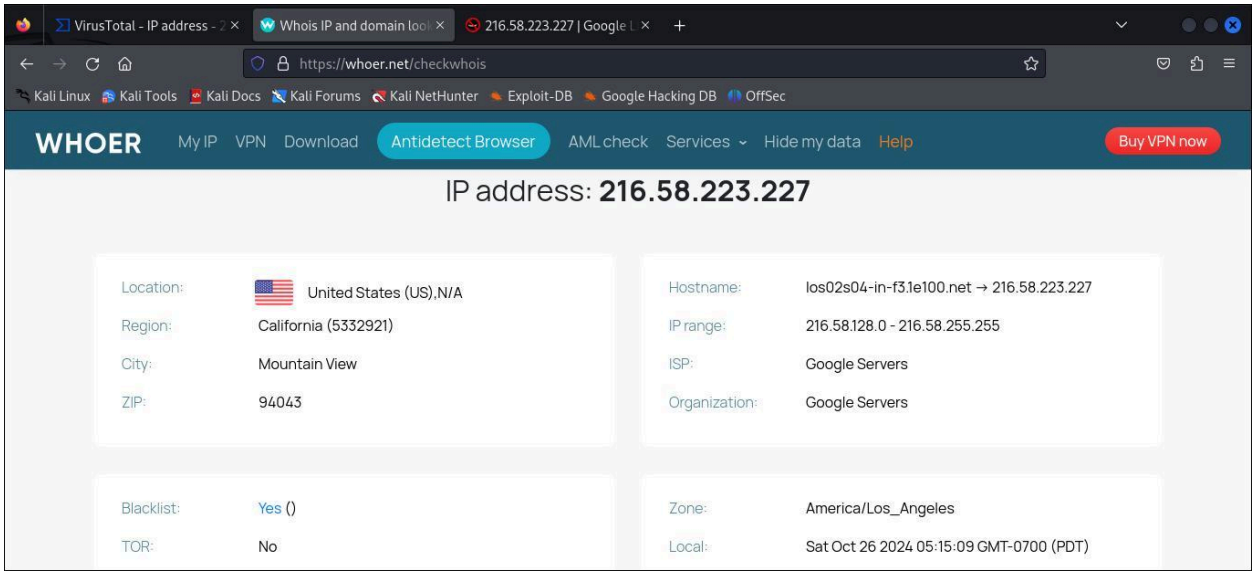


Scan result on abuseipdb

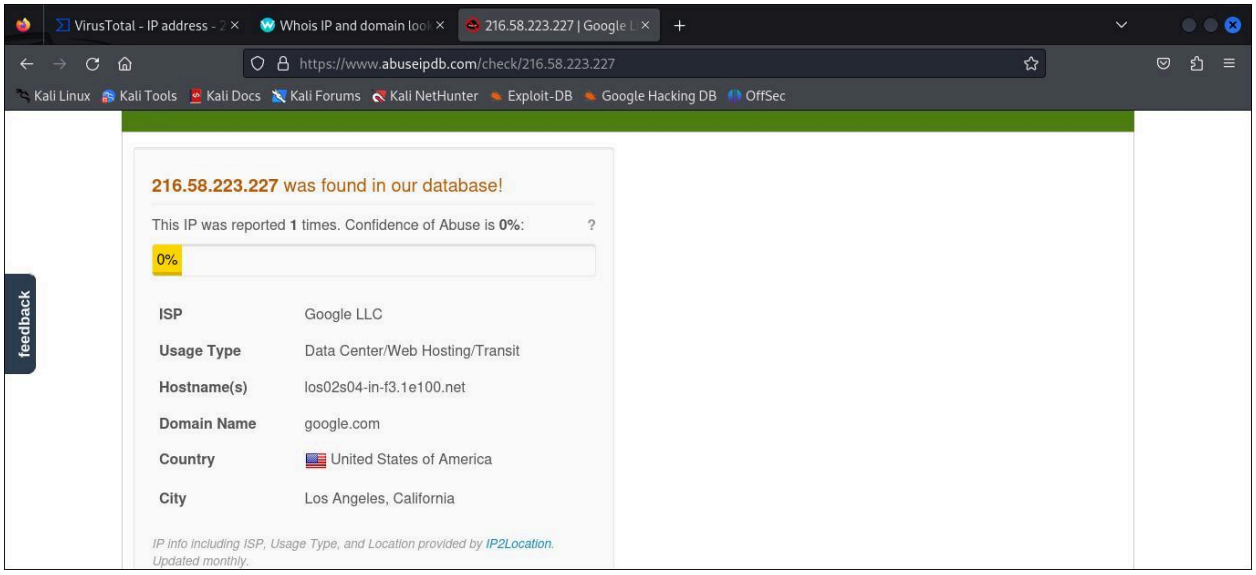
IP address 216.58.223.227



Scan result on virustotal showing this IP was self-assigned to Google

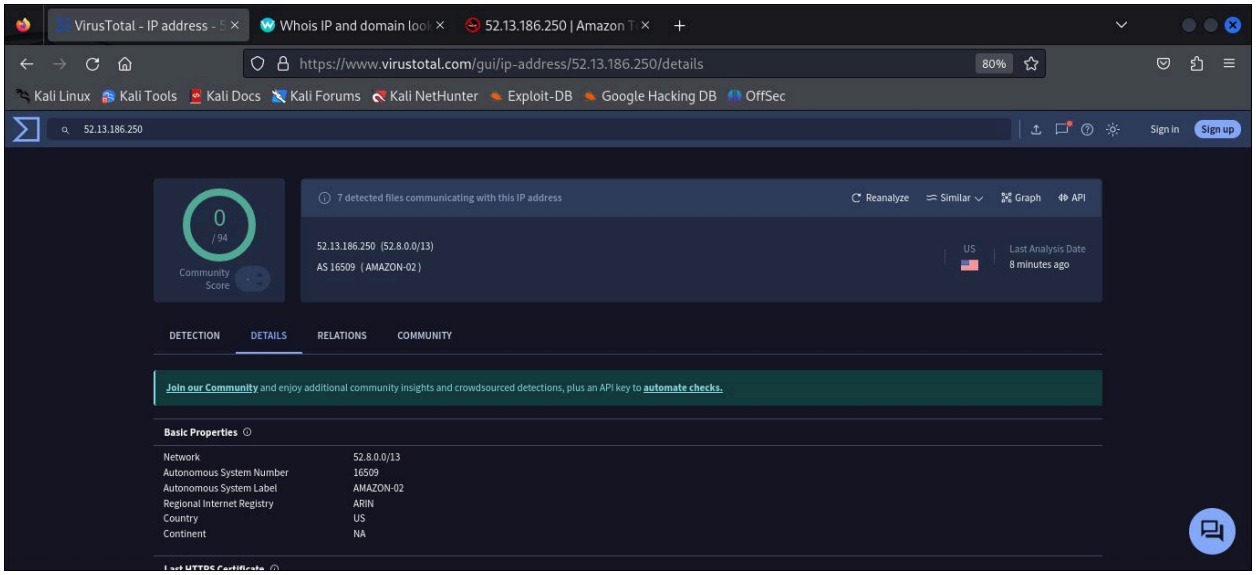


Scan result on whoer.net

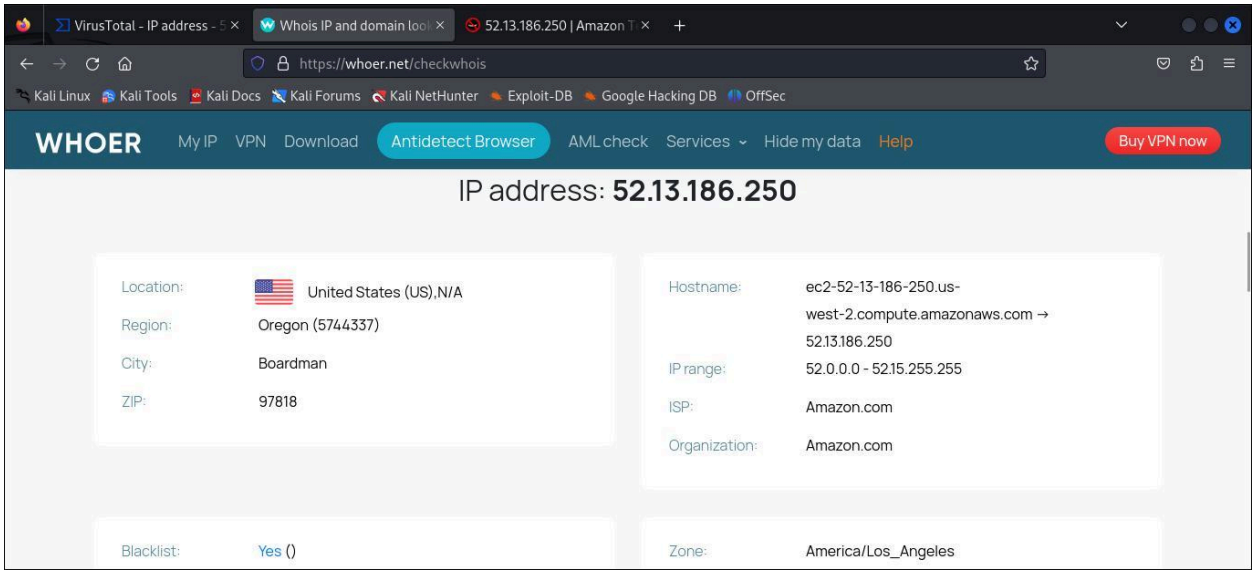


Scan result on abuseipdb

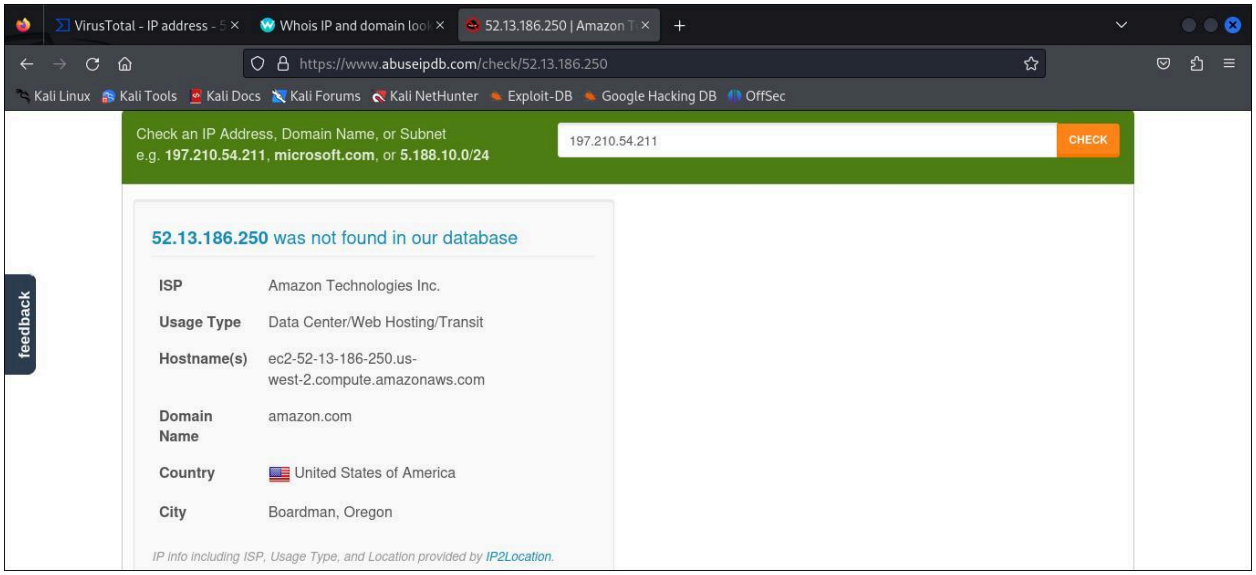
IP address 53.13.186.250



Scan result on virustotal showing this IP address belongs to Amazon

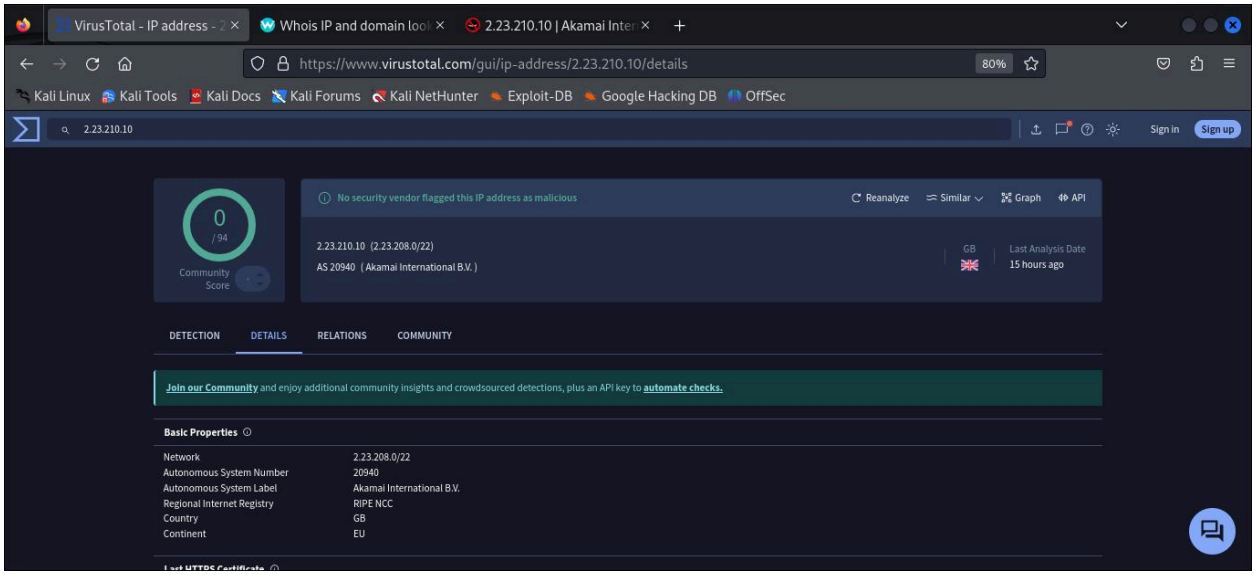


Scan result on whoer.net

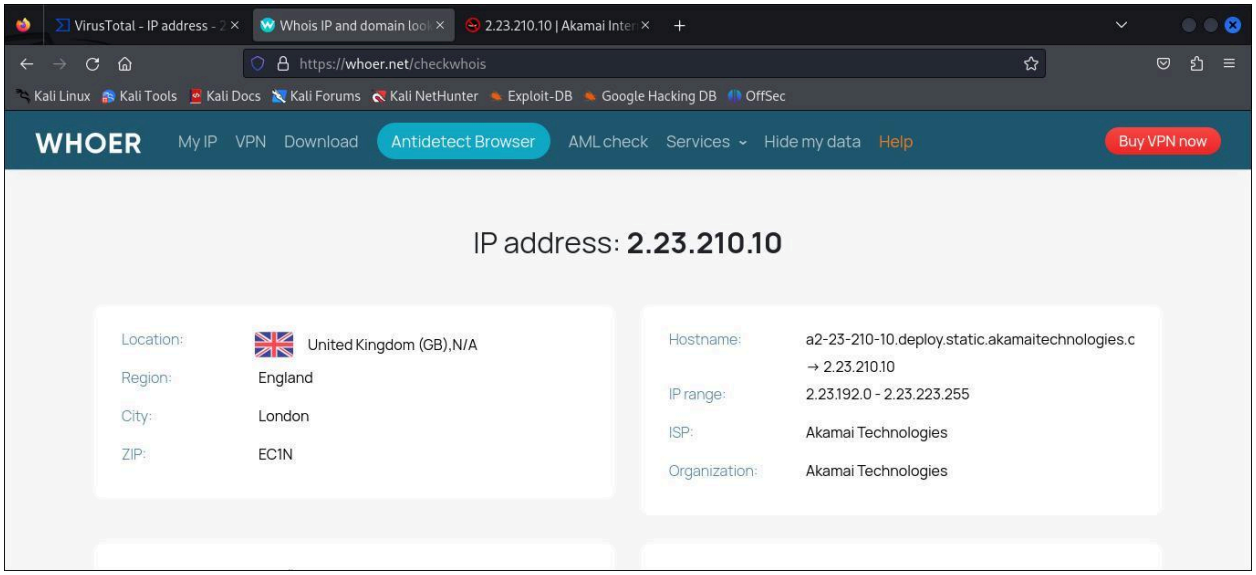


Scan result on abuseipdb

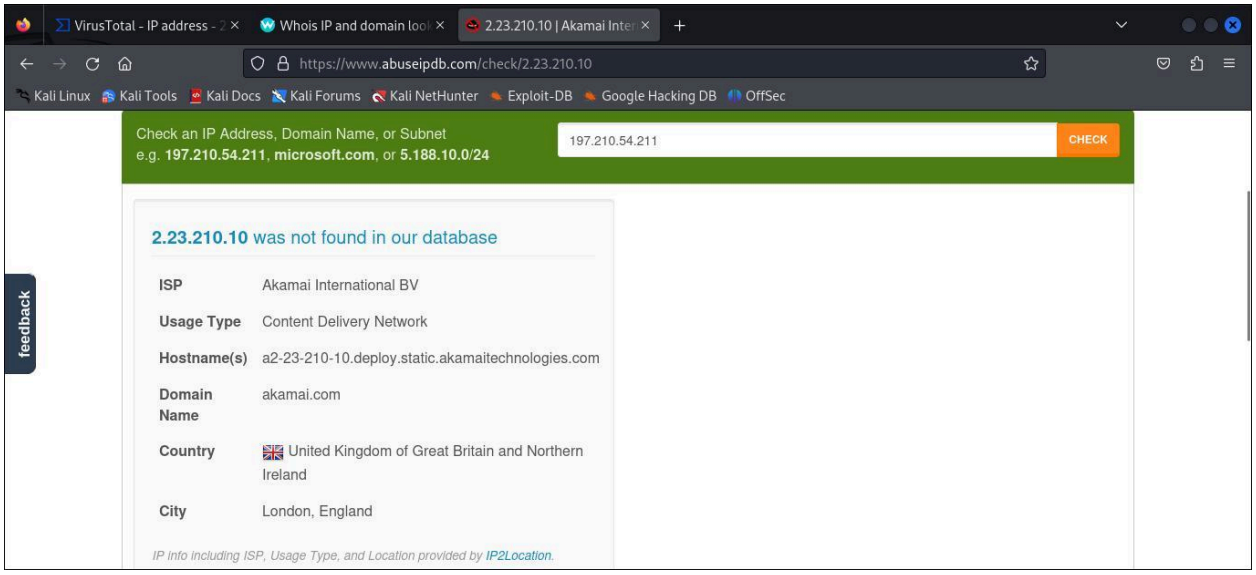
IP address 2.23.210.10



Scan result on virustotal showing this IP address belongs to Akamal International

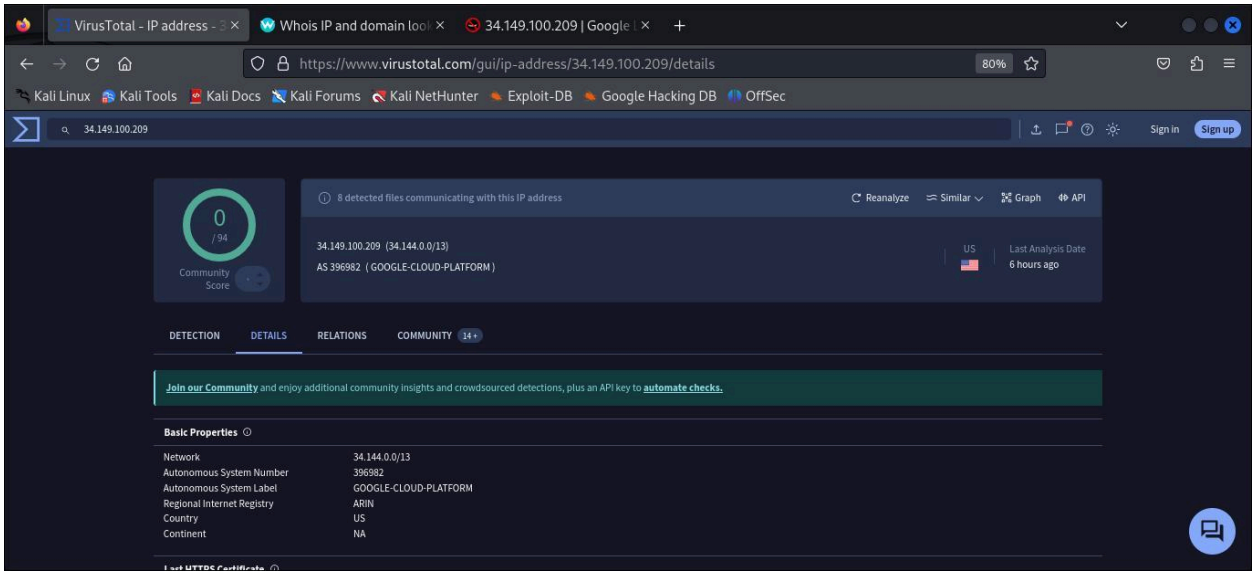


Scan result on whoer.net

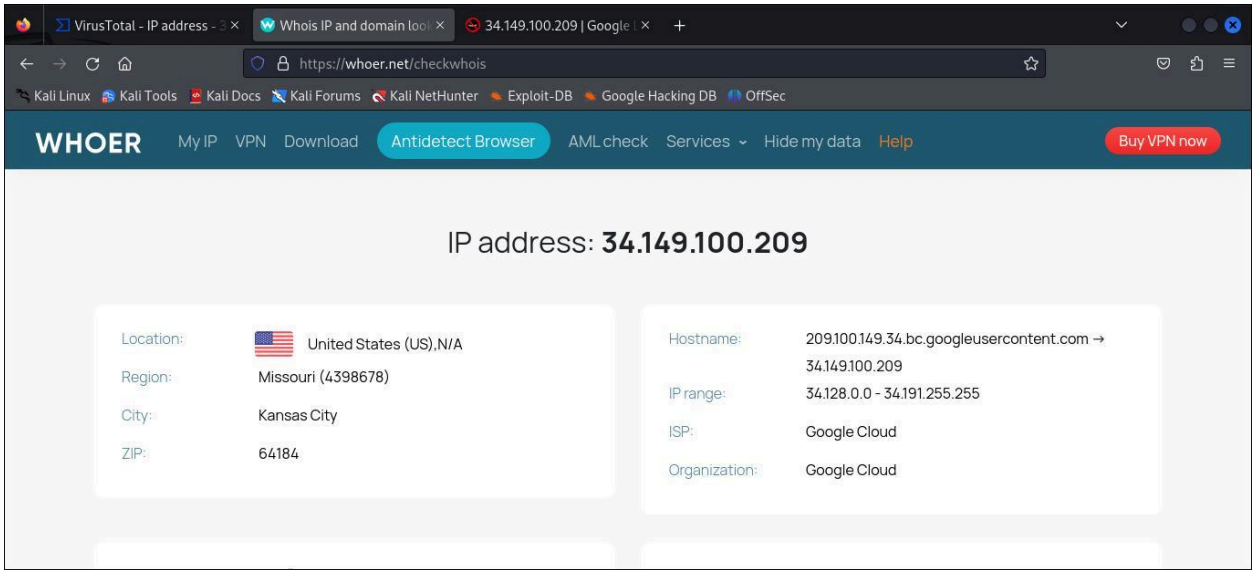


Scan result on abuseipdb

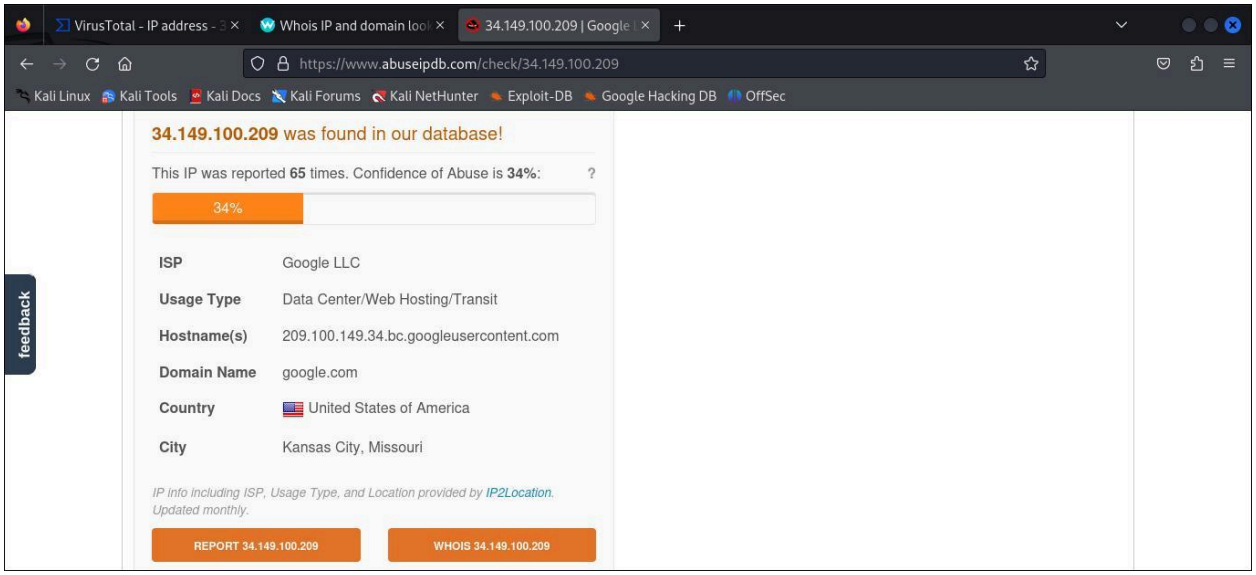
IP address 34.149.100.209



Scan result on virustotal showing this IP belongs to Google cloud

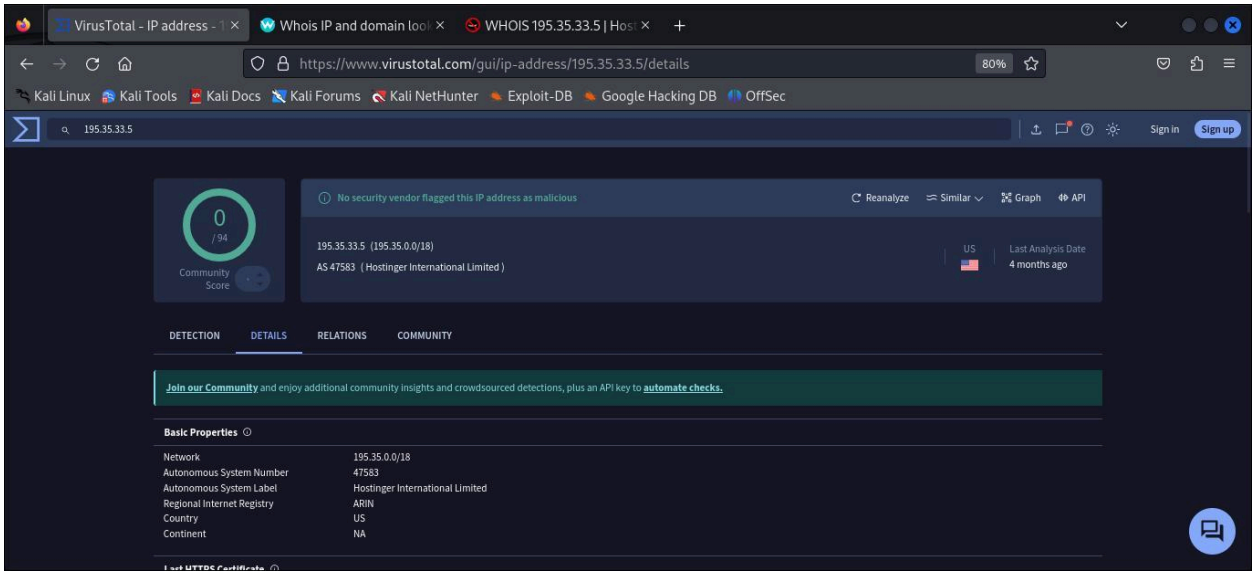


Scan result on whoer.com

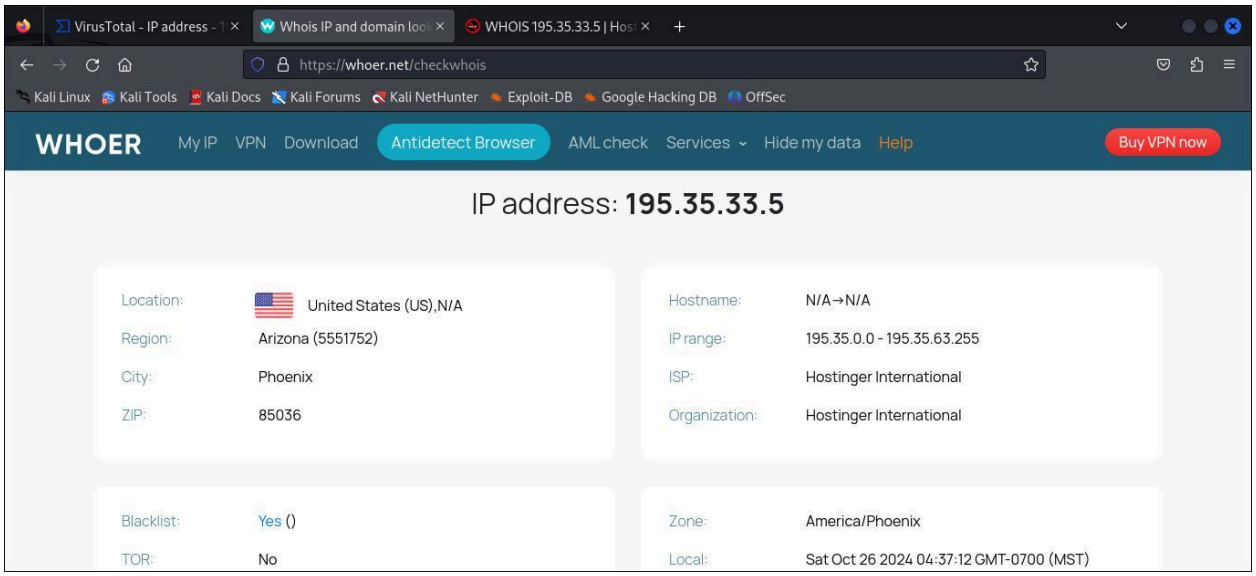


Scan result on abuseipdb

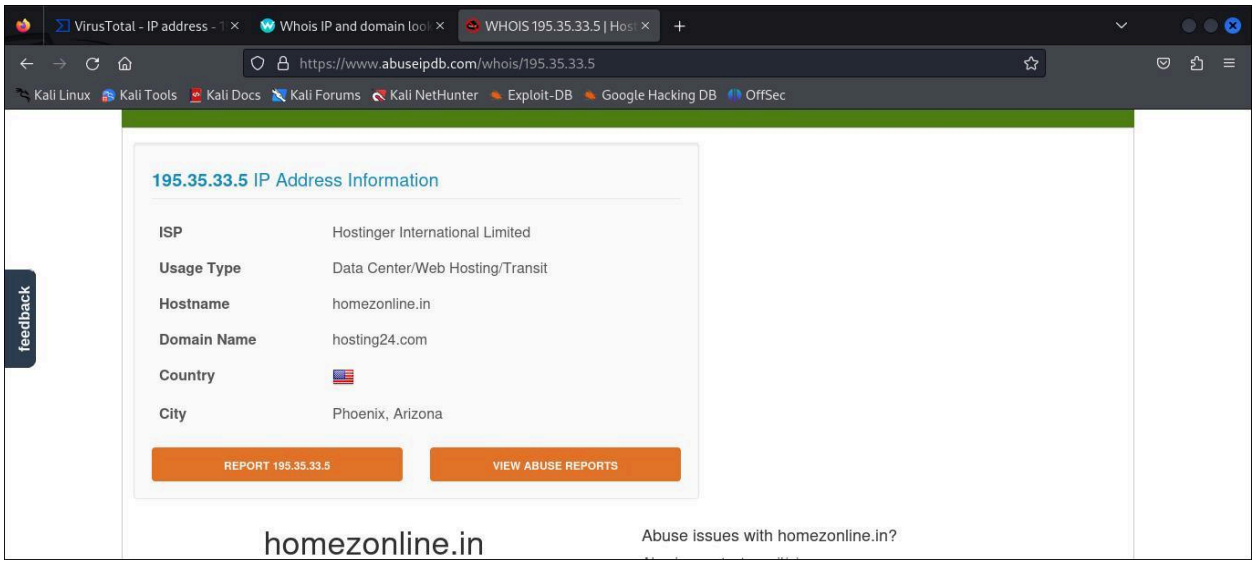
IP address: 195.35.33.5



Scan result on virustotal showing this IP belongs to Hostinger International which is the hosting provider for blockchainunn.org

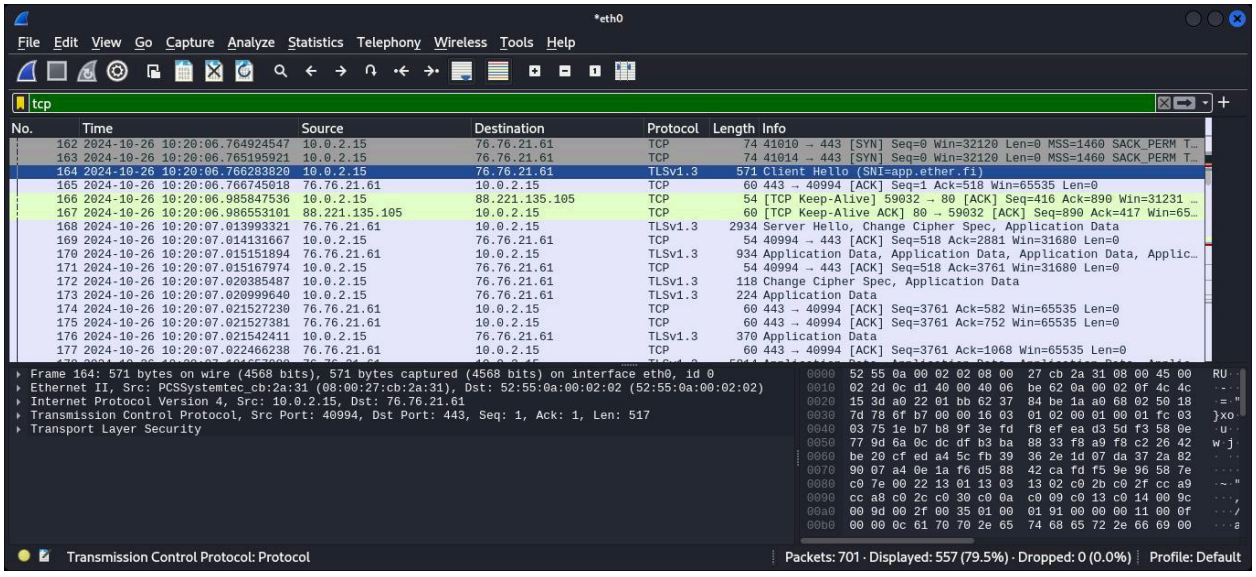


Scan result on whoer.net



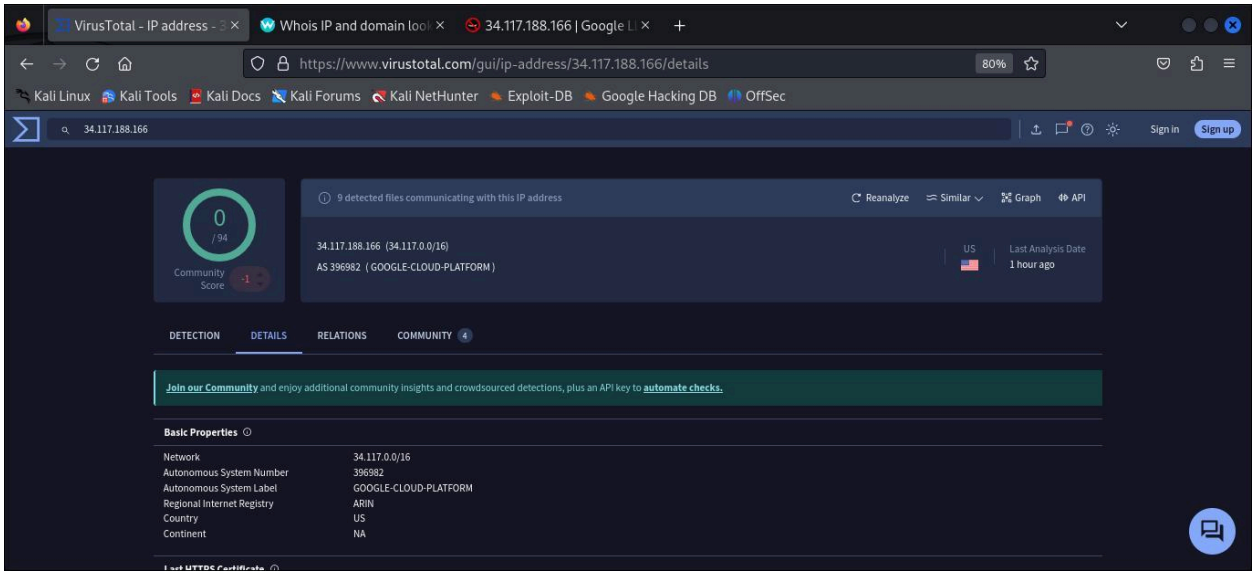
Scan result of the IP on whoer.net

B. For app.ether.fi

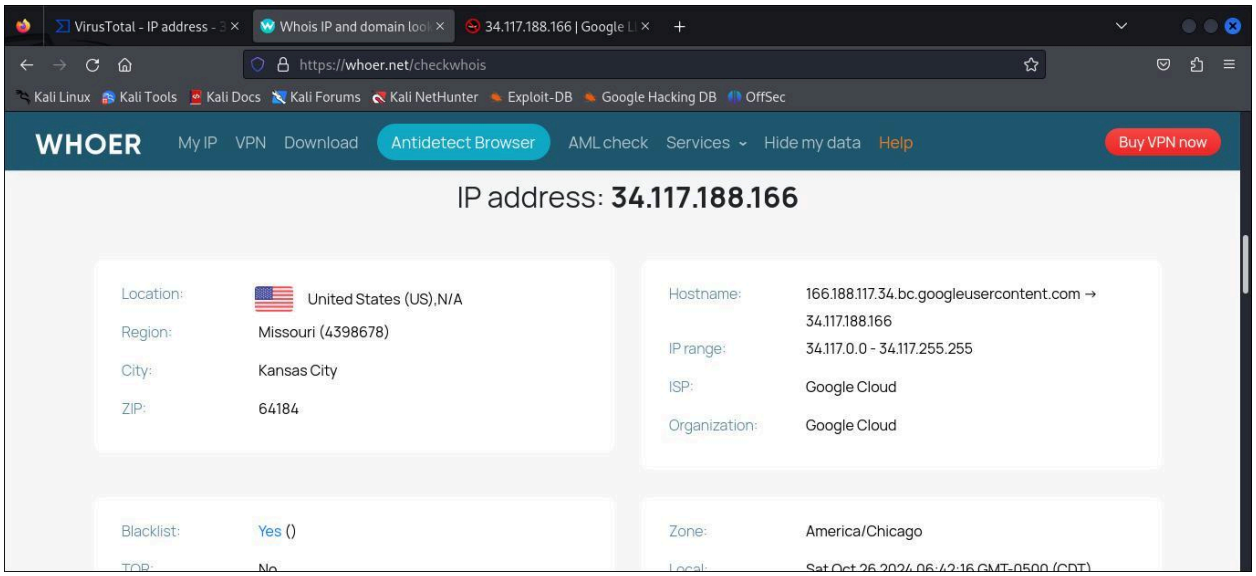


An Overview of some packet details captured on Wireshark during the access to app.ether.fi

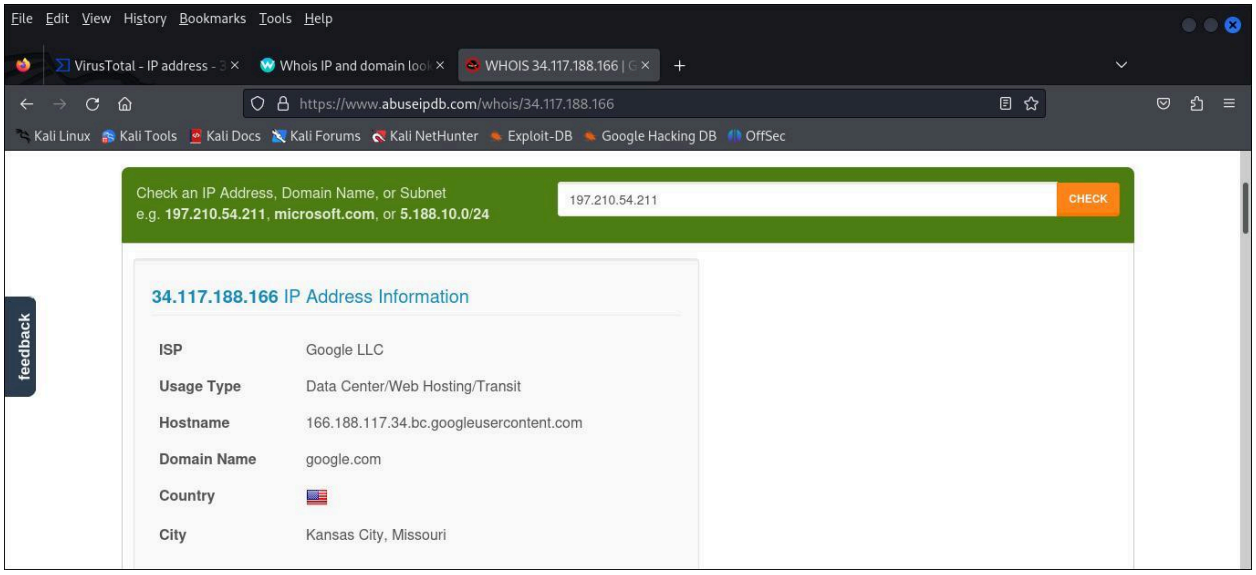
IP address 34.117.188.166



Scan result on virustotal showing this IP belongs to Google cloud

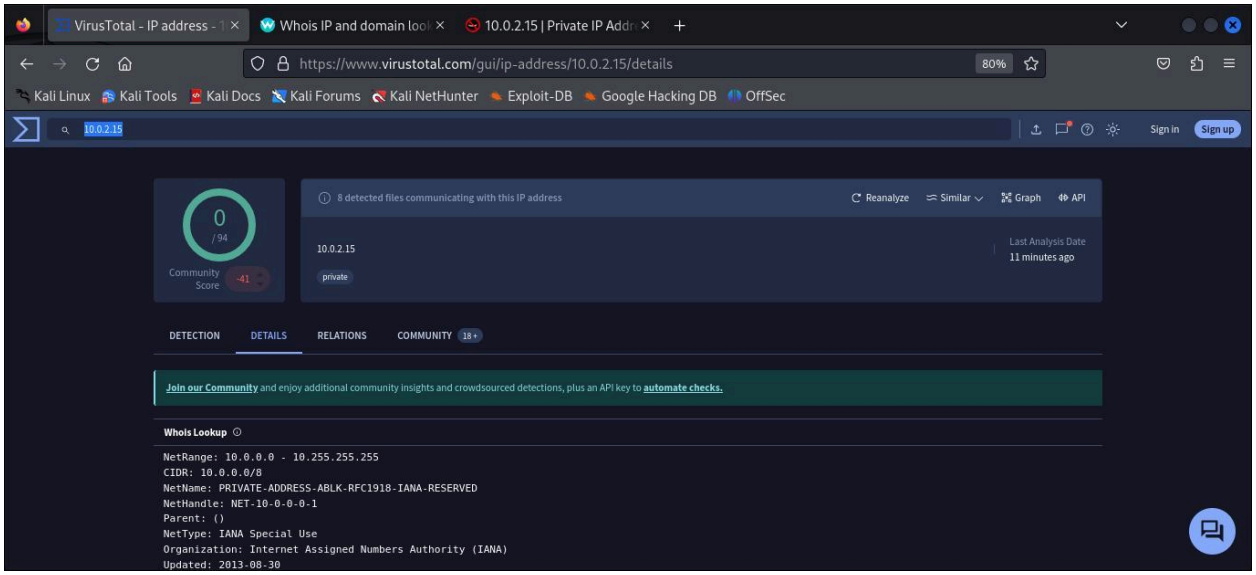


Scan on whoer.net

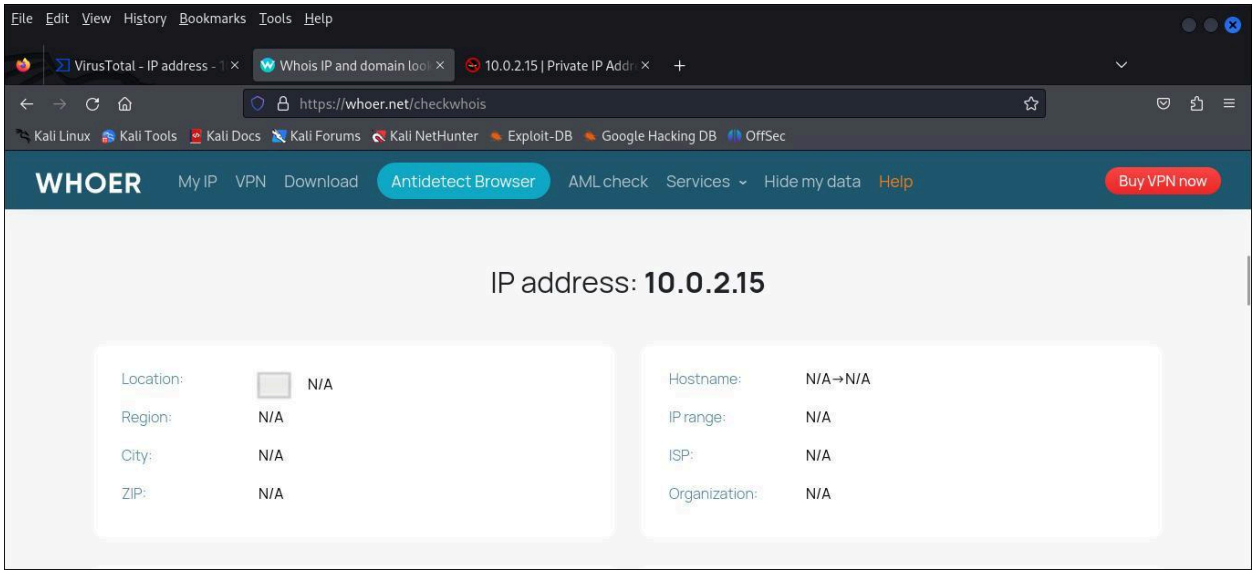


Scan result on abuseipdb

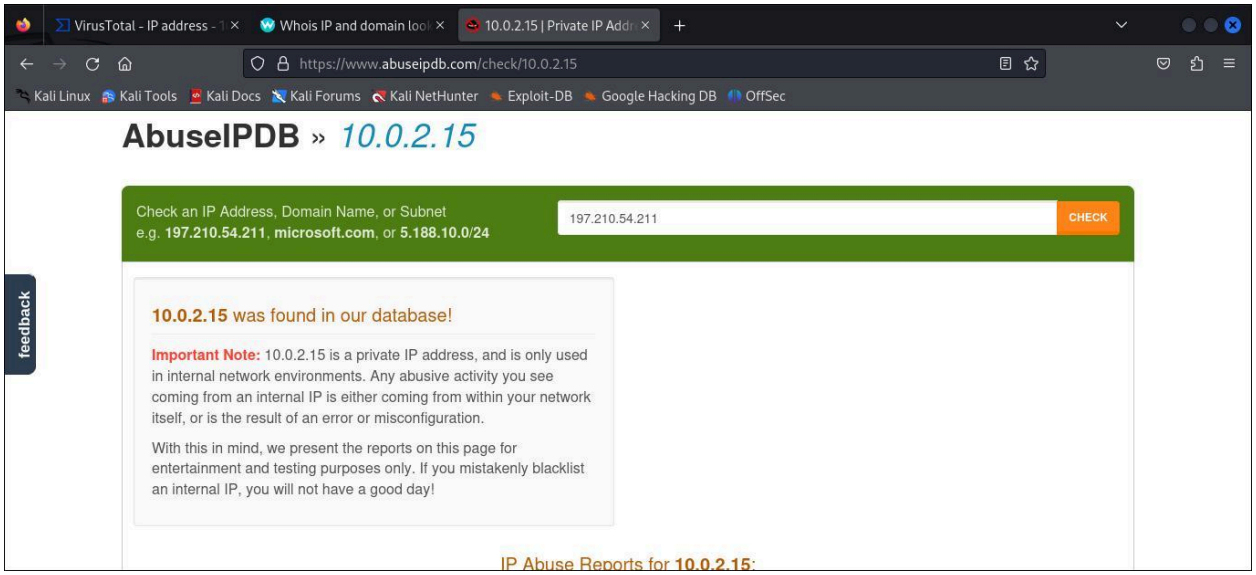
IP address 10.0.2.15



Scan result on virustotal showing this IP is private

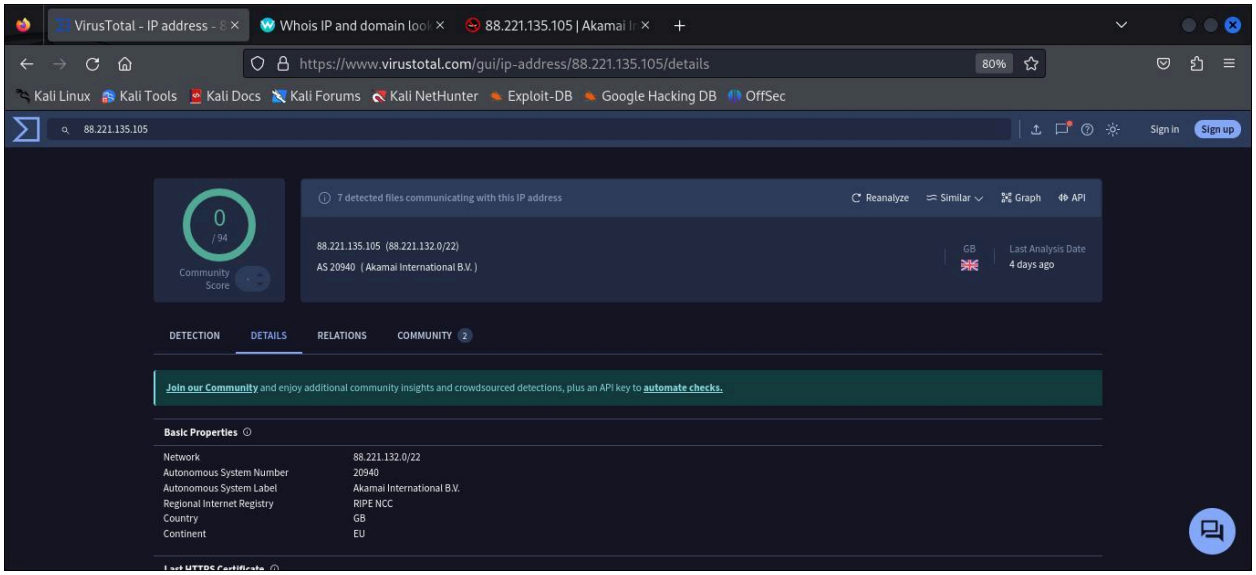


Scan result on whoer.net

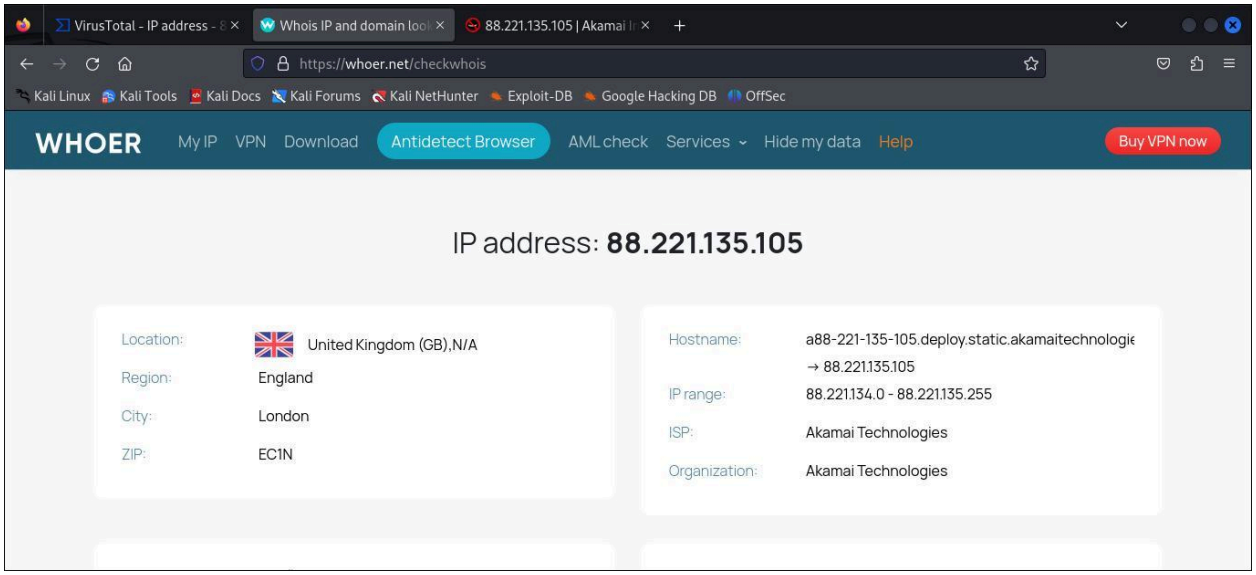


Scan result on abuseipdb

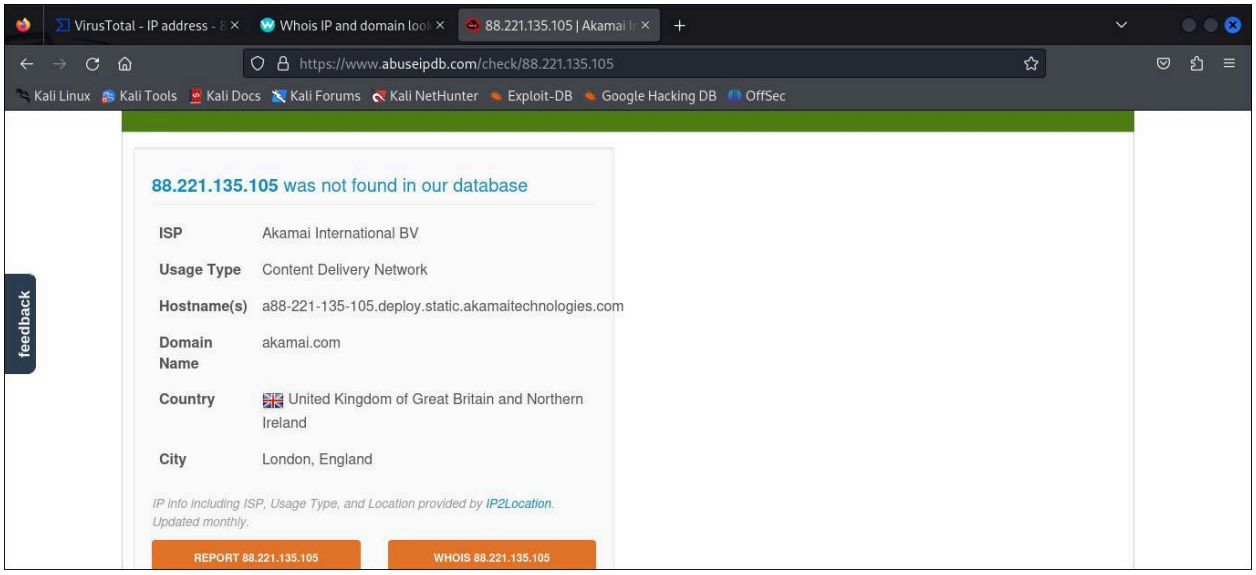
IP address 88.221.135.105



Scan result on virustotal showing this IP belongs to Akamal International

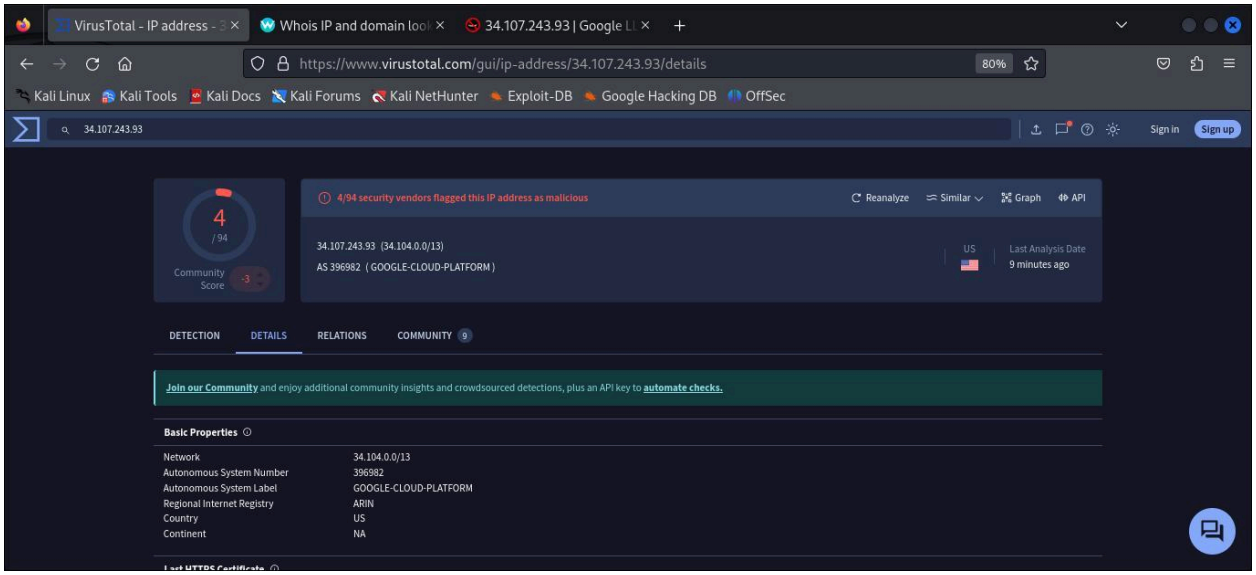


Scan result on whoer.net

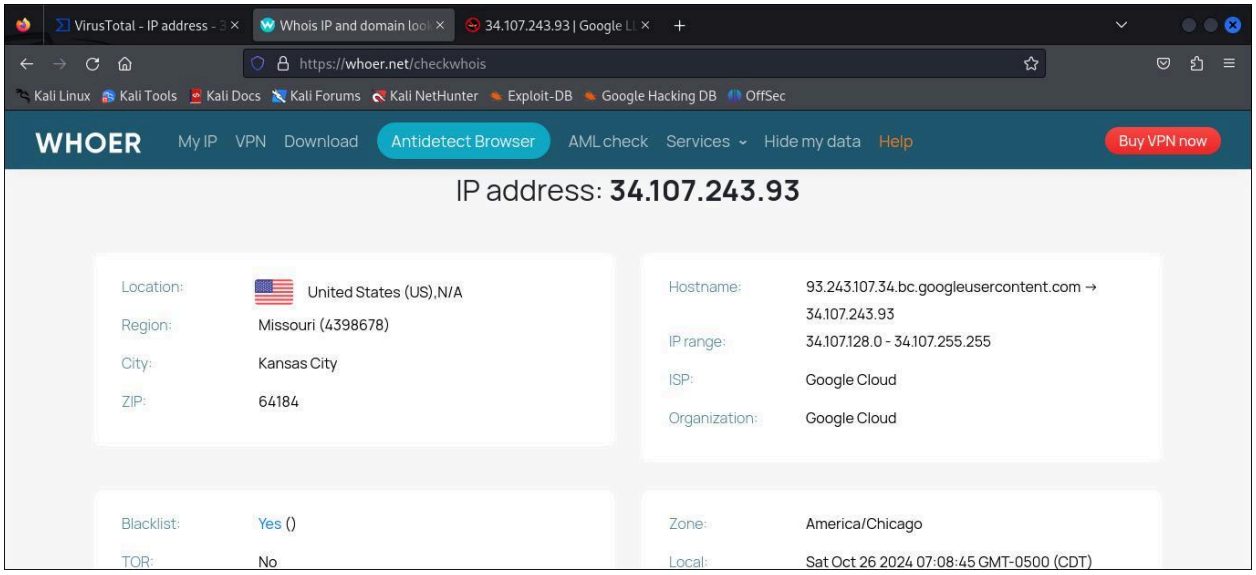


Scan result on abuseipdb

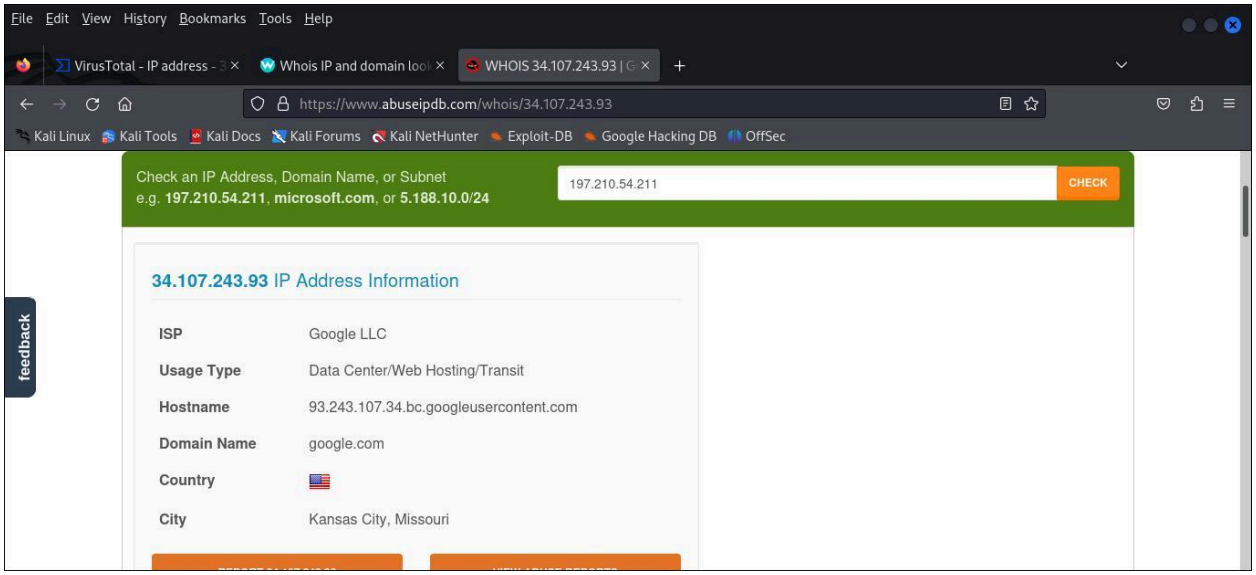
IP address 34.107.243.93



Scan result virustotal flagging this IP as malicious

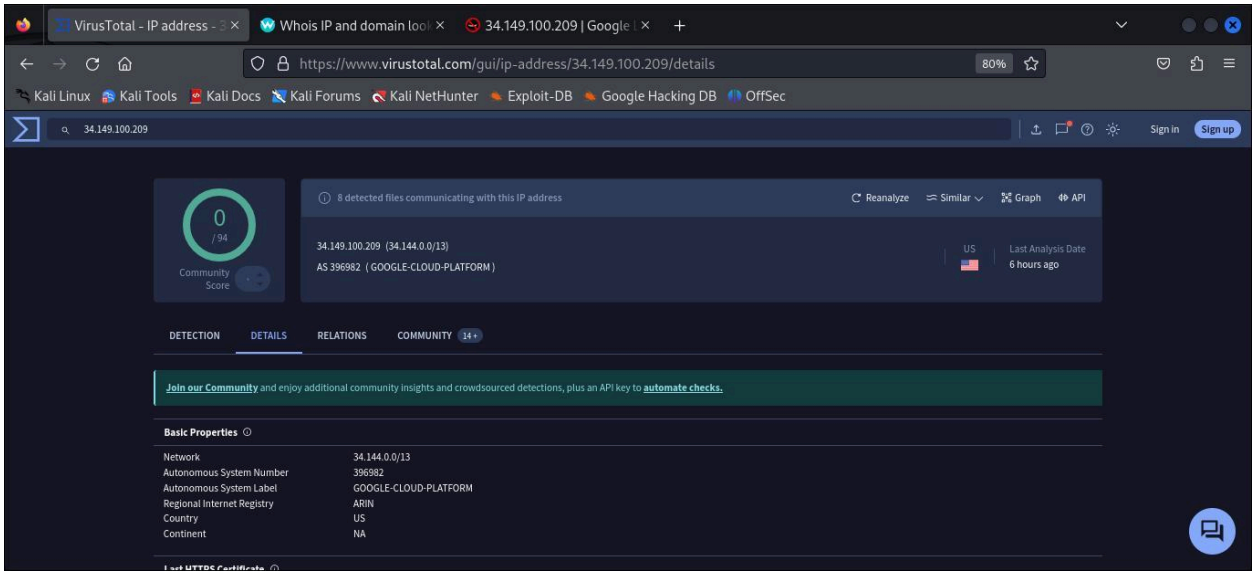


Scan result on whoer.net

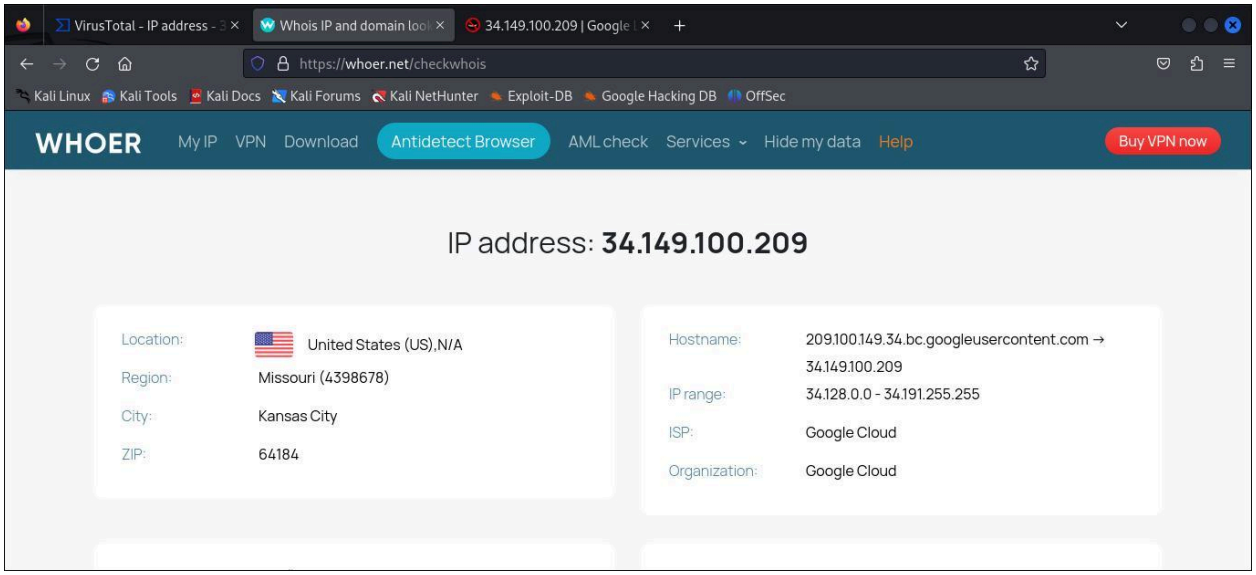


Scan result on abuseipdb

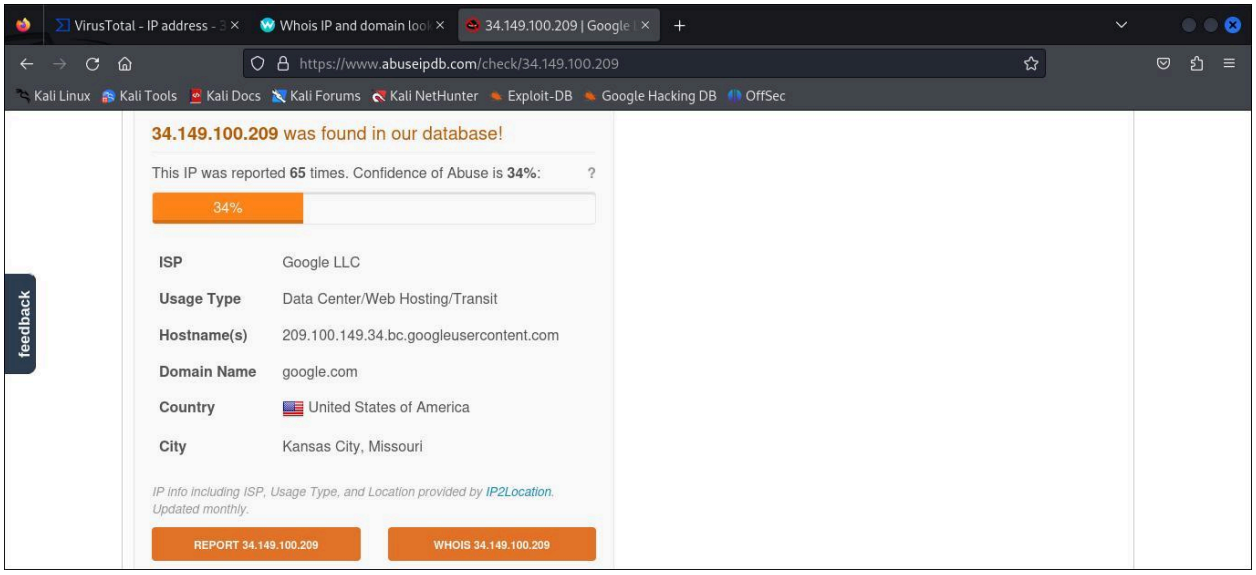
IP address 34.149.100.209



Scan result on virustotal showing this IP belongs to Google cloud

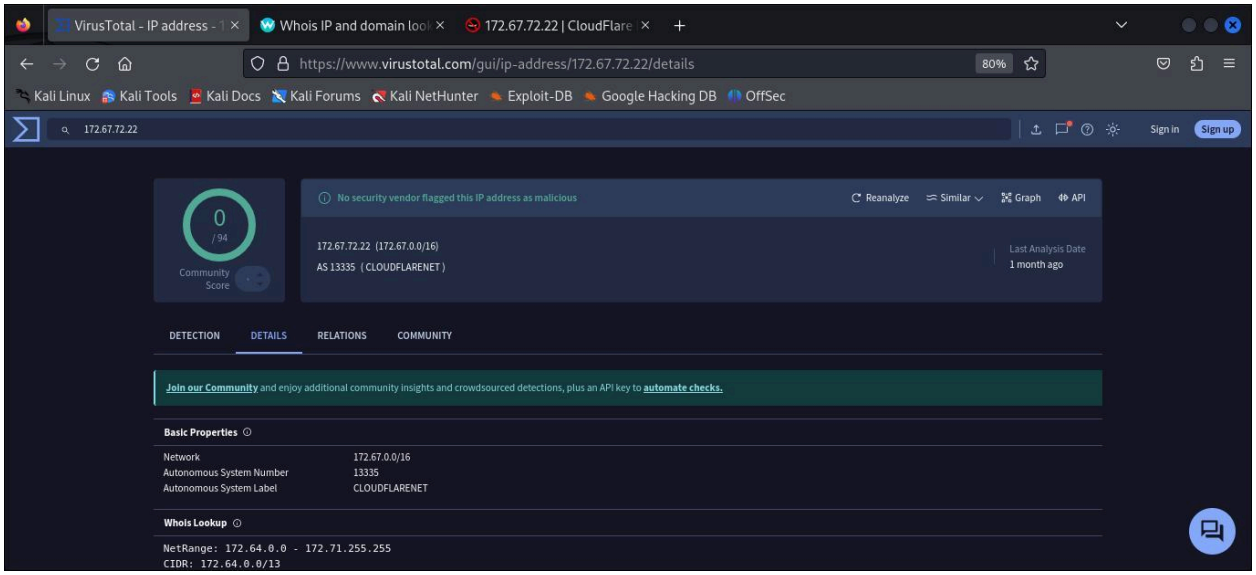


Scan result on whoer.net

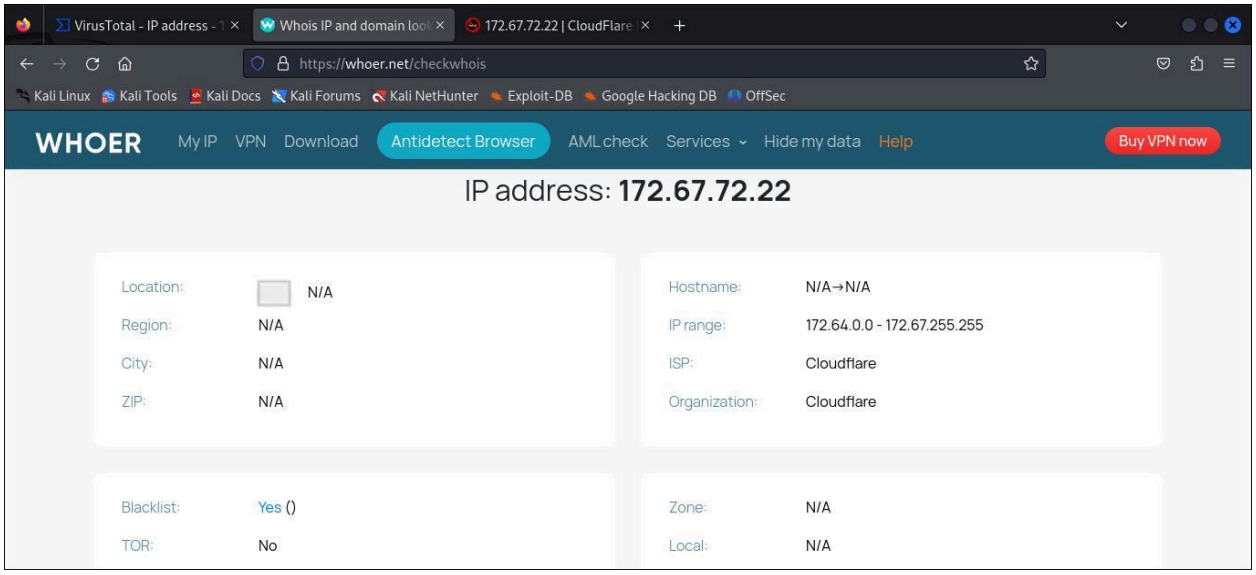


Scan result on abuseipdb

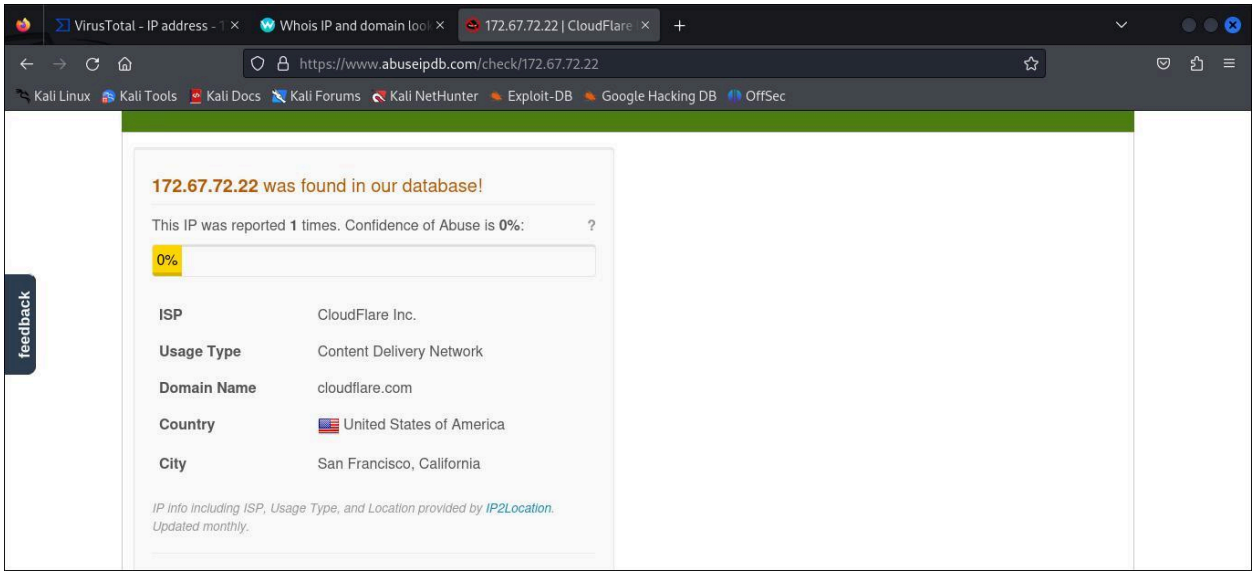
IP address 172.67.72.22



Scan result on virustotal showing this IP belongs to Cloudflarenet

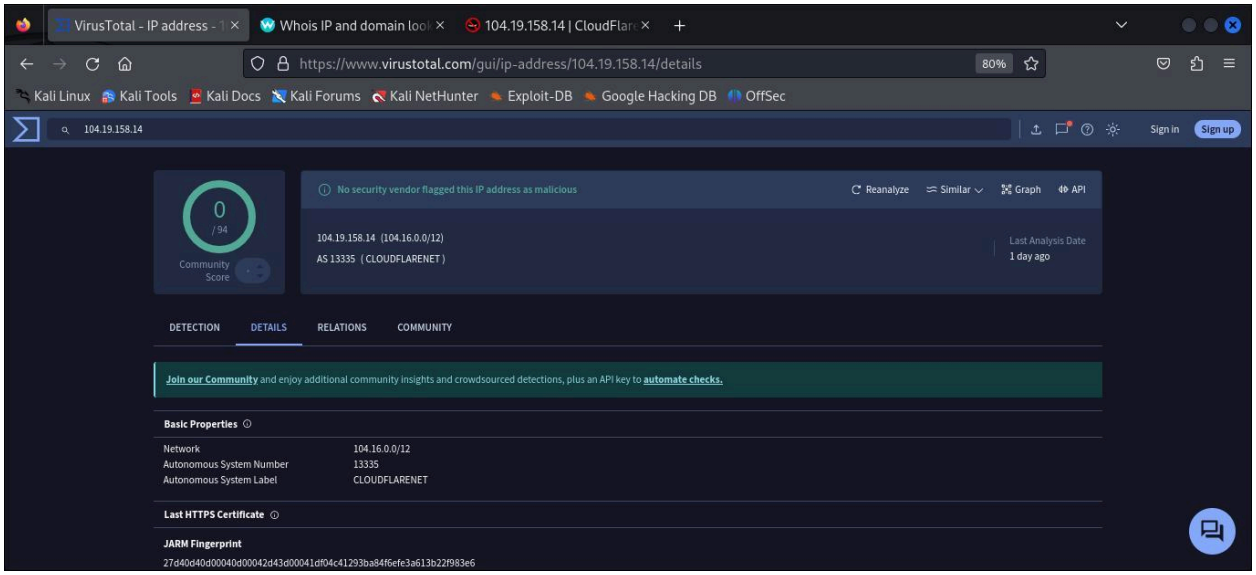


Scan result on whoer.net

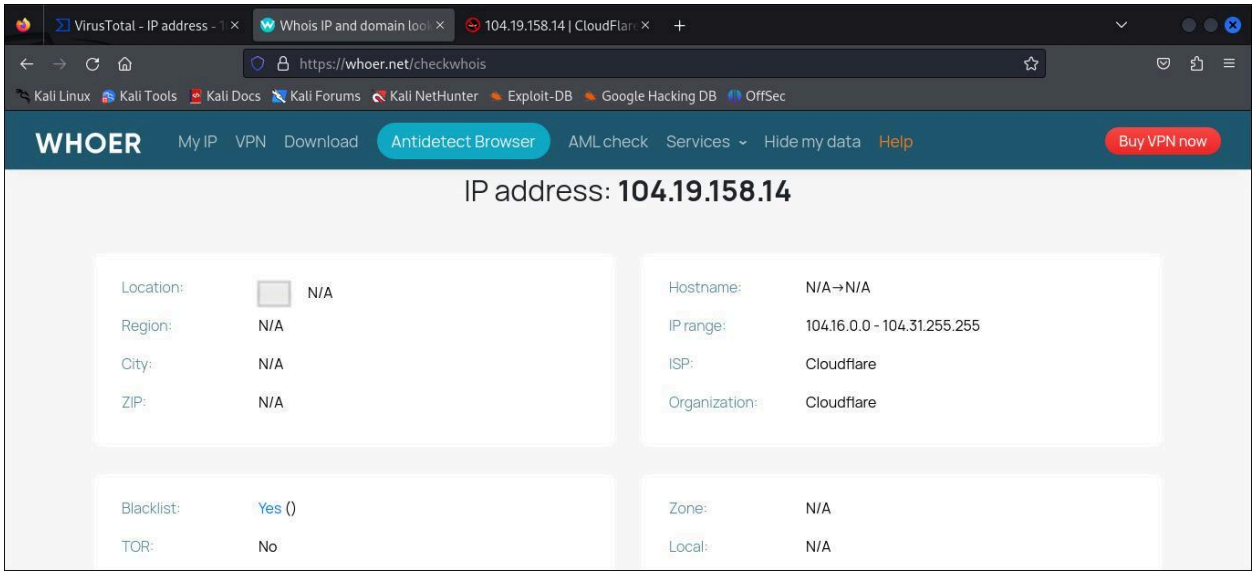


Scan result on abuseipdb

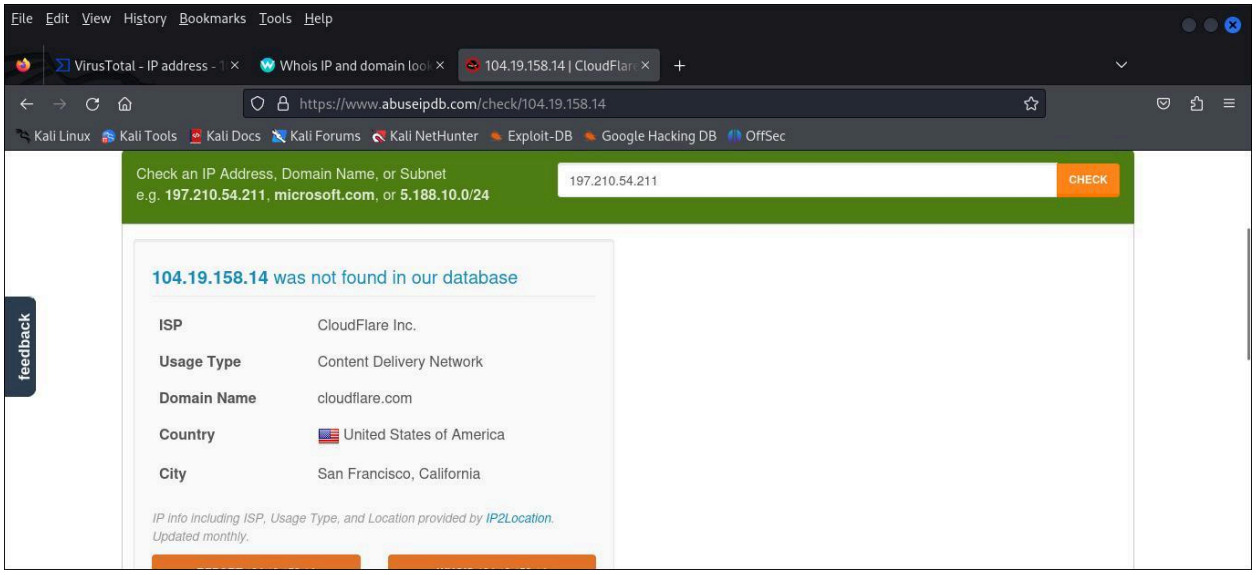
IP address 104.19.158.14



Scan result on virustotal Showing this IP belongs to Cloudflarenet

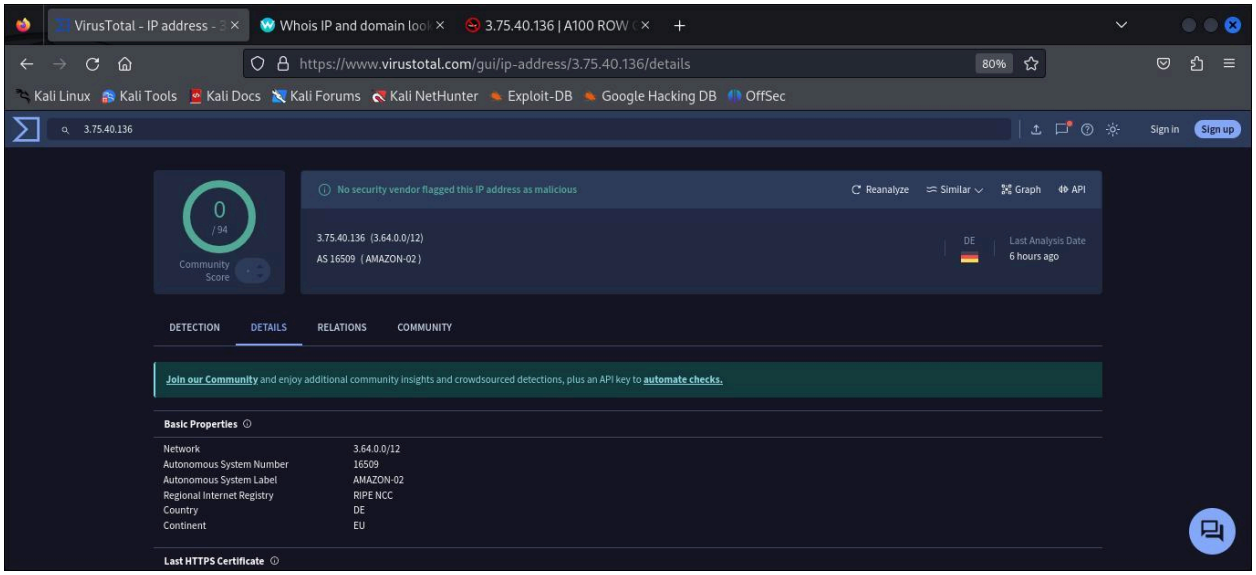


Scan result on whoer.net

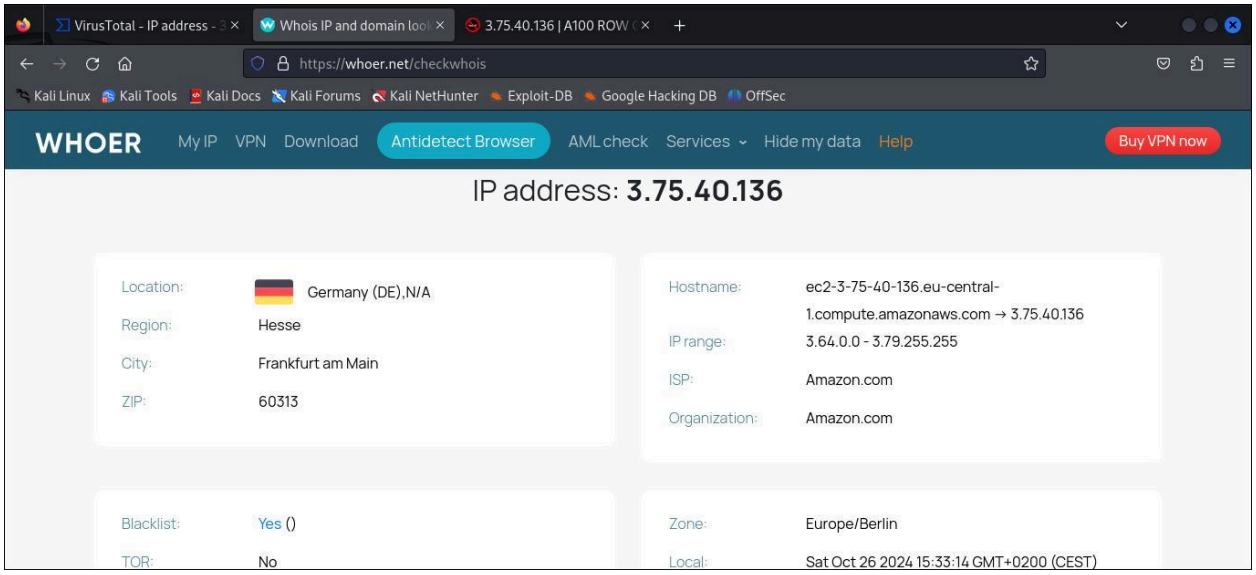


Scan result om abuseipdb

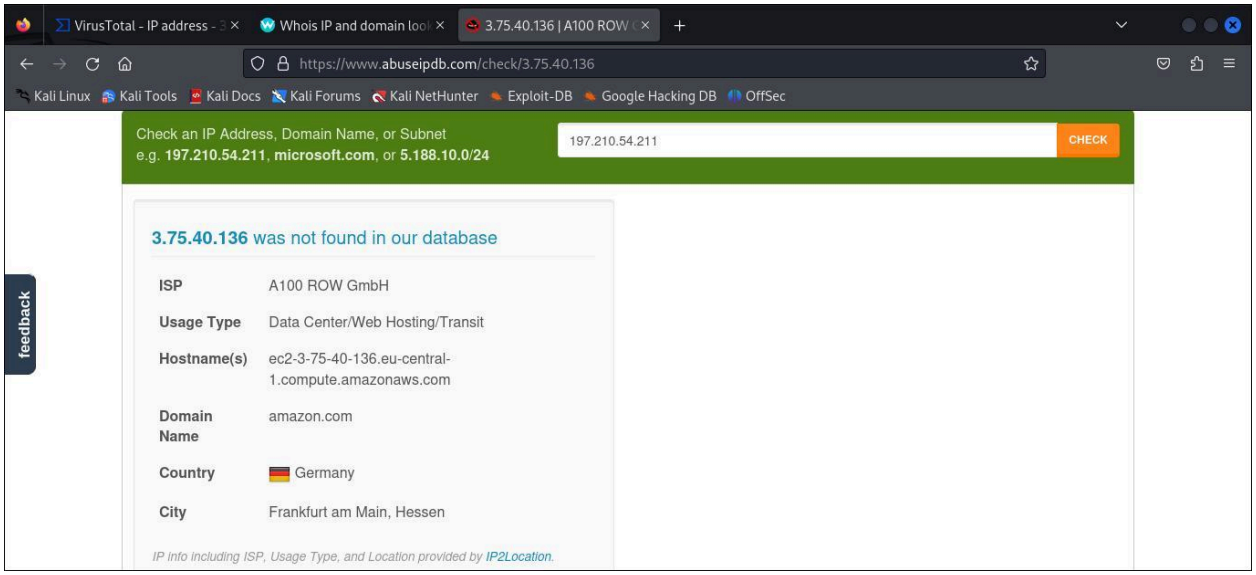
IP address 3.75.40.136



Scan result on virustotal showing this IP belongs to Amazon

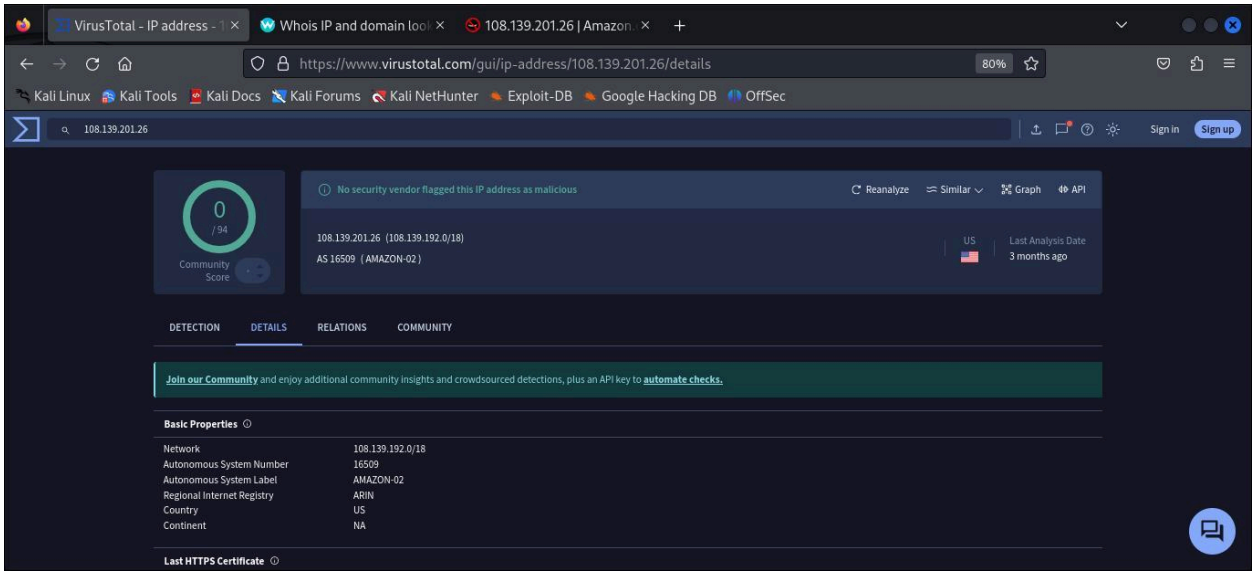


Scan result on whoer.net

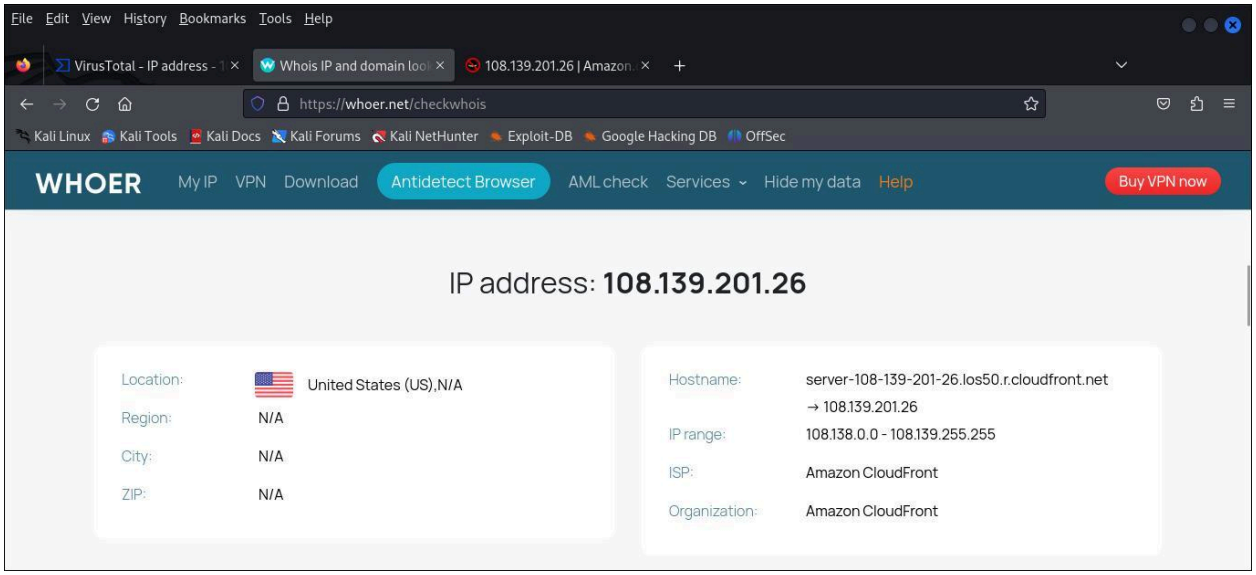


Scan result on abuseipdb

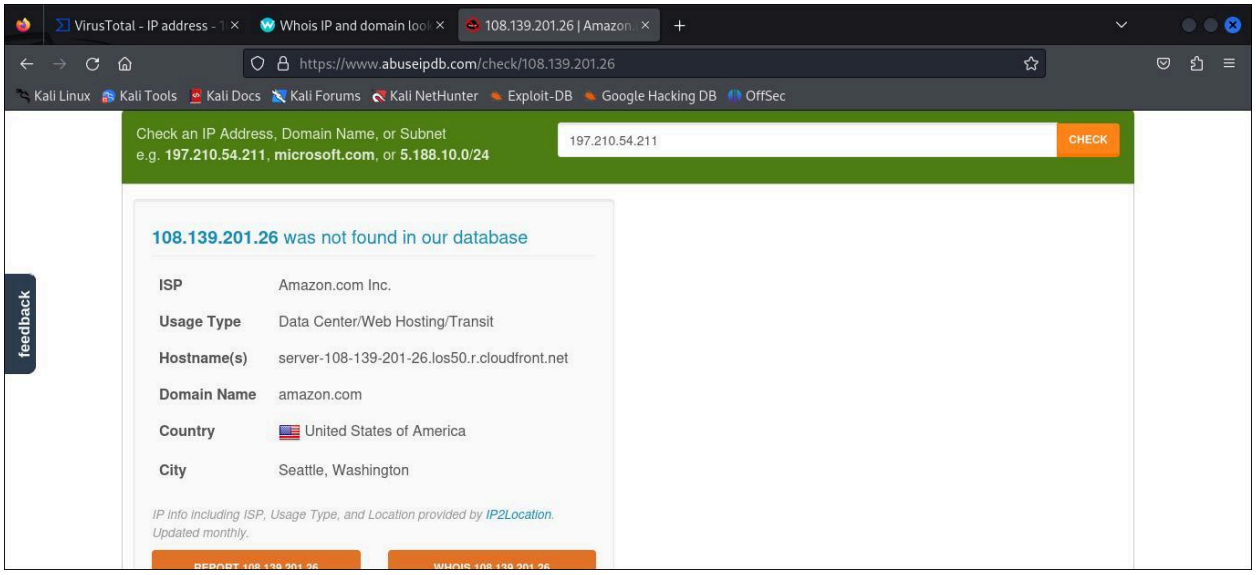
IP address 108.139.201.26



Scan result on virustotal showing this IP belongs to Amazon

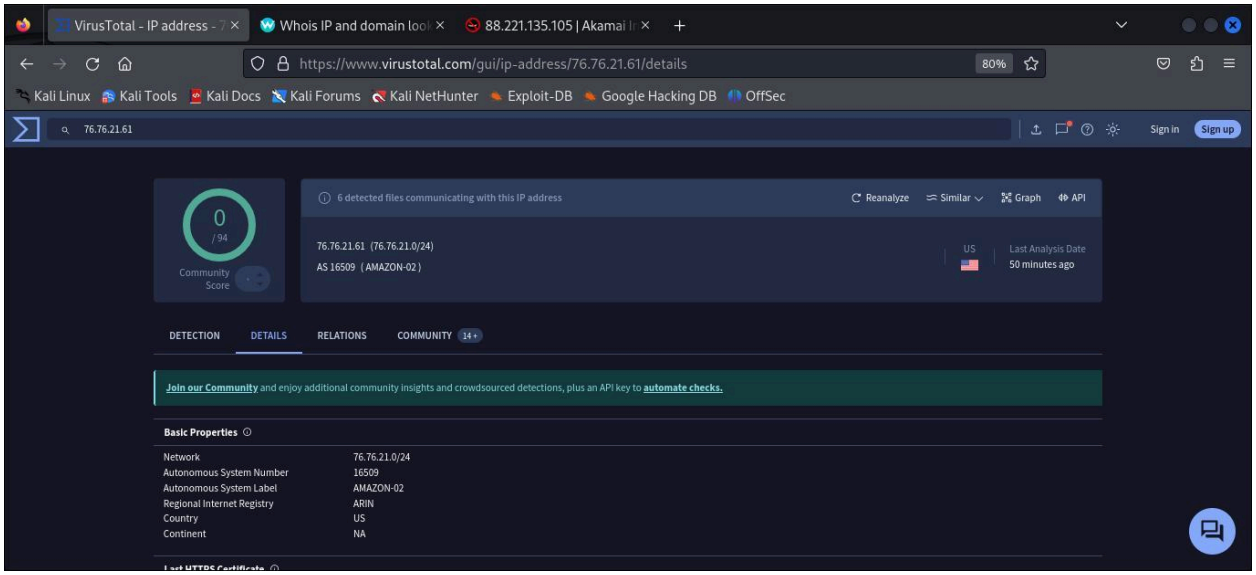


Scan result on whoer.net

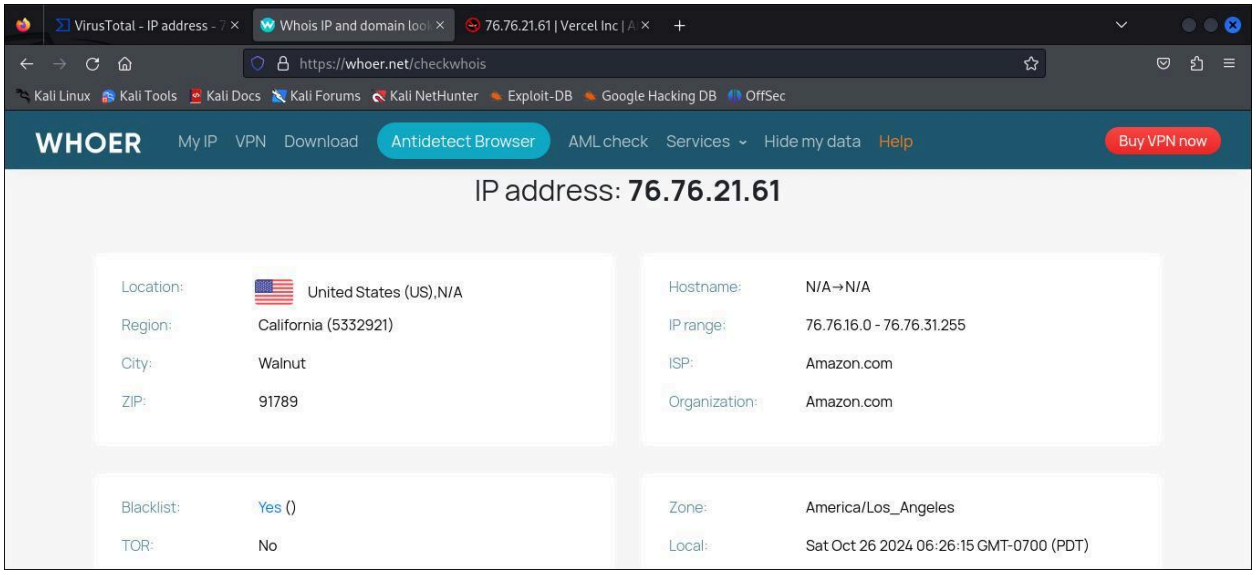


Scan result on abuseipdb

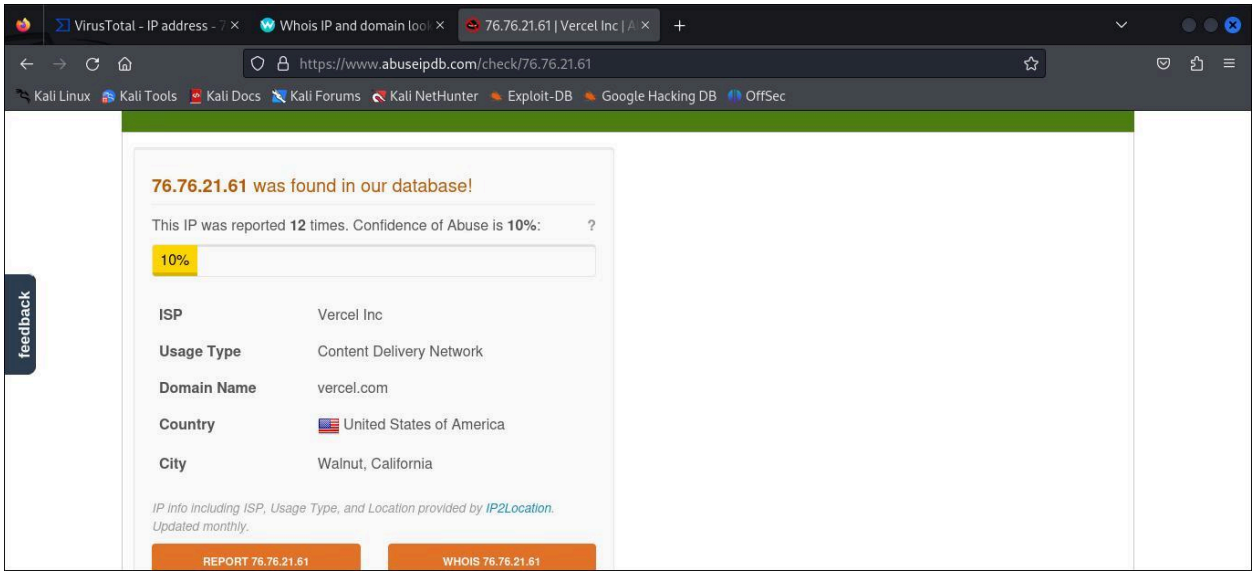
IP address 76.76.21.61



Scan result on virustotal showing this IP belongs to Amazon



Scan result on whoer.net



Scan result on abuseipdb showing the ISP to be Vercel Inc. and Domain name to be vercel.com. This shows that app.ether.fi is hosted on Vercel which in turn runs on Amazon Web Service.

RECOMMENDATION

1. Blocking of the malicious IP identified. This will stop any further communication with that IP and protect the network from potential threats.

2. Setting up continuous monitoring will help catch any unusual IP activity, especially from new or unknown addresses. This proactive approach ensures quick detection of suspicious activities.

3. Configuring alerts will keep the security team's of both domains informed of potential threats as they arise, allowing them to respond promptly and maintain network security.

CONCLUSION

While the majority of IP addresses in these captures are safe, the single malicious IP found ought to be further investigated by the owners (Google). The shared IPs appearing in both domains also indicate that blockchainunn.org and app.ether.fi share a common network pathway. Therefore, regular monitoring can help reduce vulnerabilities and keep the network more secure.