CAPTURING OF NETWORK TRAFFIC USING TCPDUMP

BY

SOMKENE RICHARD

20th OCTOBER, 2024

EXECUTIVE SUMMARY

In this report, tcpdump was used to capture packets sent to and received from Instagram.com, one of the domains communicating over port 443. Further analysis of the destination IP address (102.132.101.174) obtained from the packets was conducted to check for any malicious flagging, using tools such as VirusTotal.com, Whoer.net, and Abuseipdb which further showed the IP address to be malicious-free.

INTRODUCTION

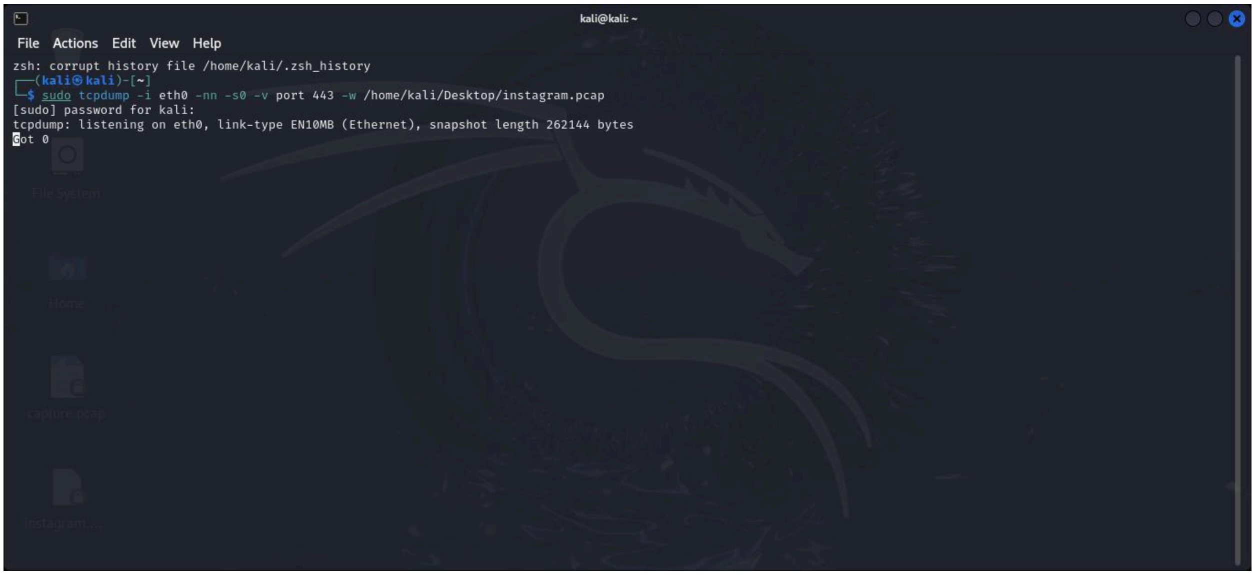
TCPdump is a powerful network packet analyzer that allows users to capture and analyze network traffic. It is a valuable tool for network administrators, cybersecurity professionals, and developers to troubleshoot network issues, monitor traffic, and identify potential security threats.

This tool is compatible with Linux operating systems. To run packet captures on a Windows operating system, a virtual machine (VM) environment is used, with Kali Linux running inside the VM.

TOOLS

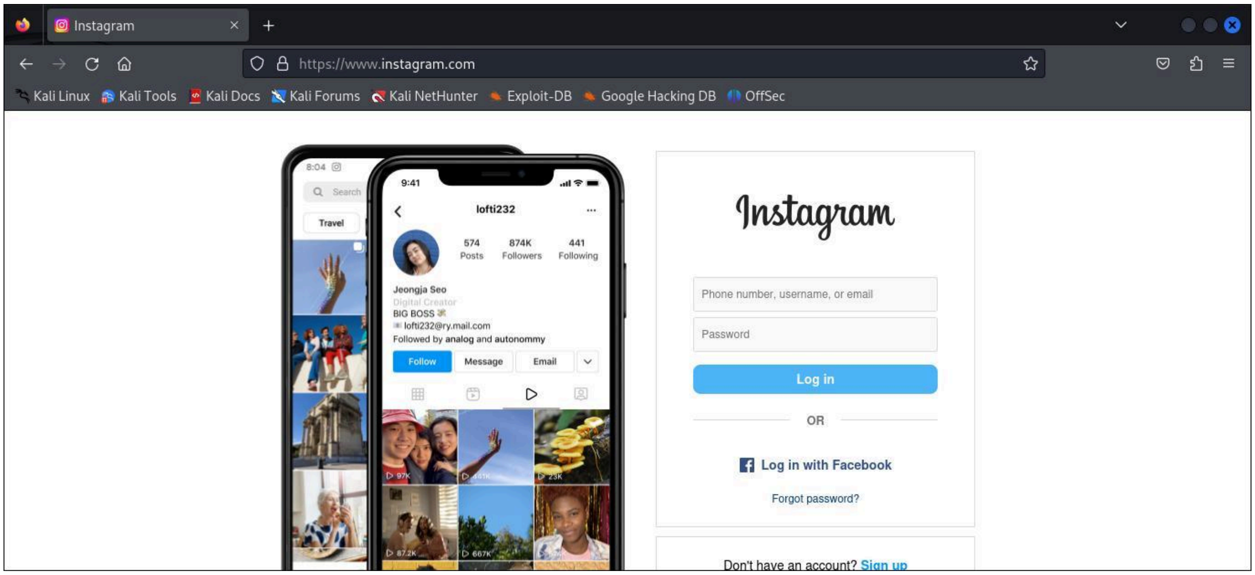
1. Kali linux
2. Tcpdump
3. Wireshark
4. Whoer.net
5. Virustotal
6. Abuseipdb

ANALYSIS

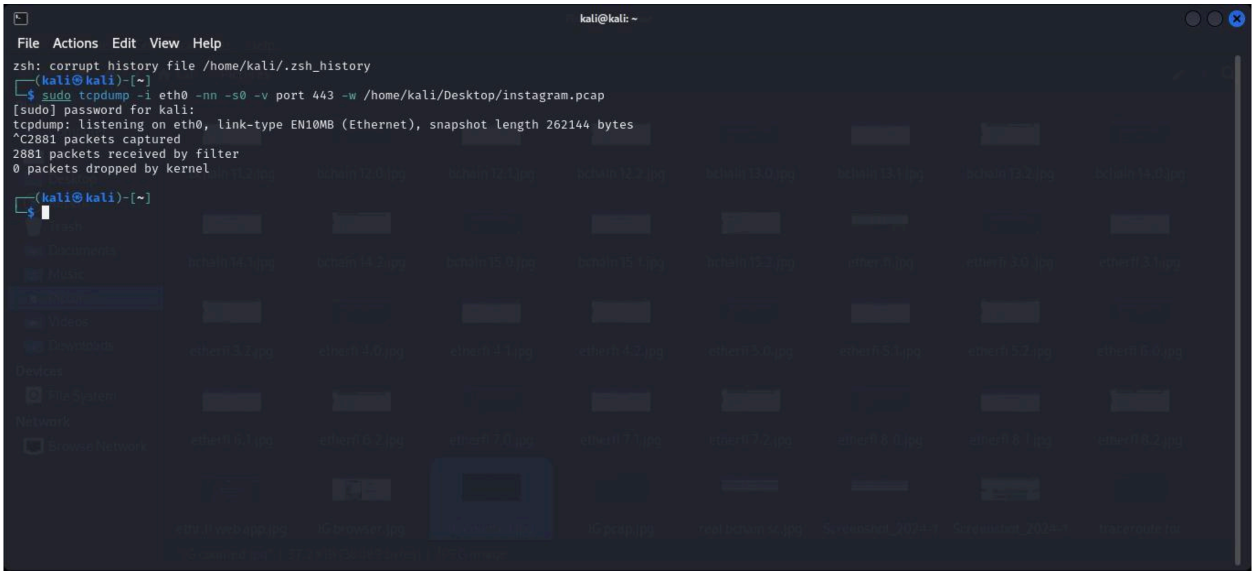


```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth0 -nn -s0 -v port 443 -w /home/kali/Desktop/instagram.pcap
[sudo] password for kali:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
Got 0
```

The figure above shows the initiation of the tcpdump command, including the port, path, and format in which the packet file would be saved as



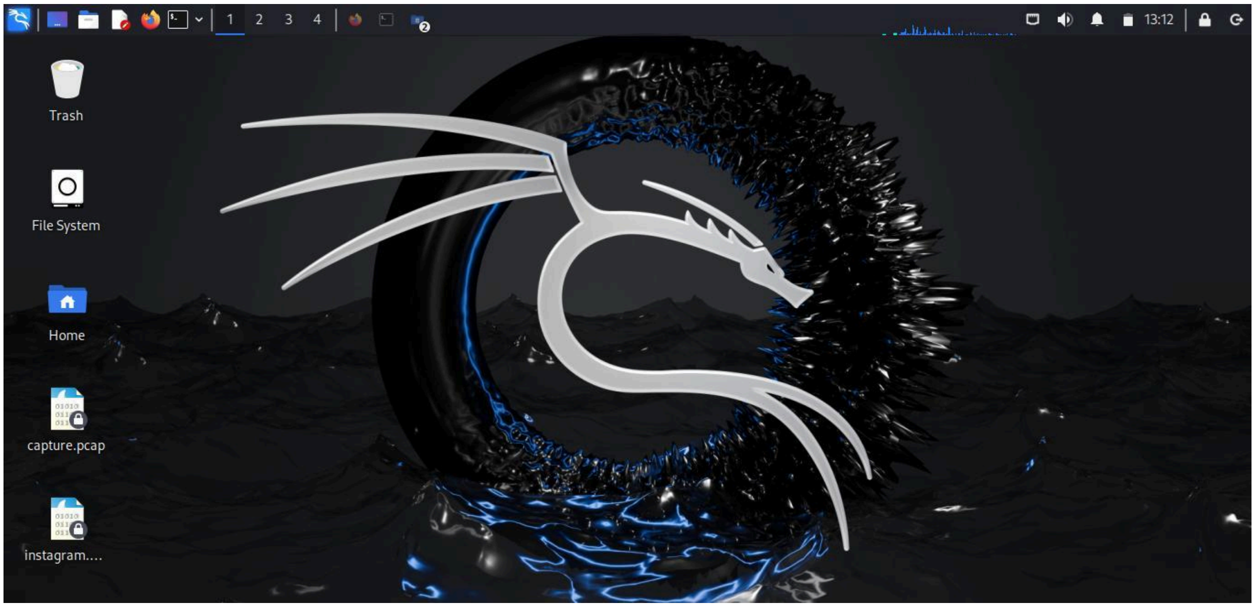
After initiating the command, Instagram.com was accessed using the Firefox browser



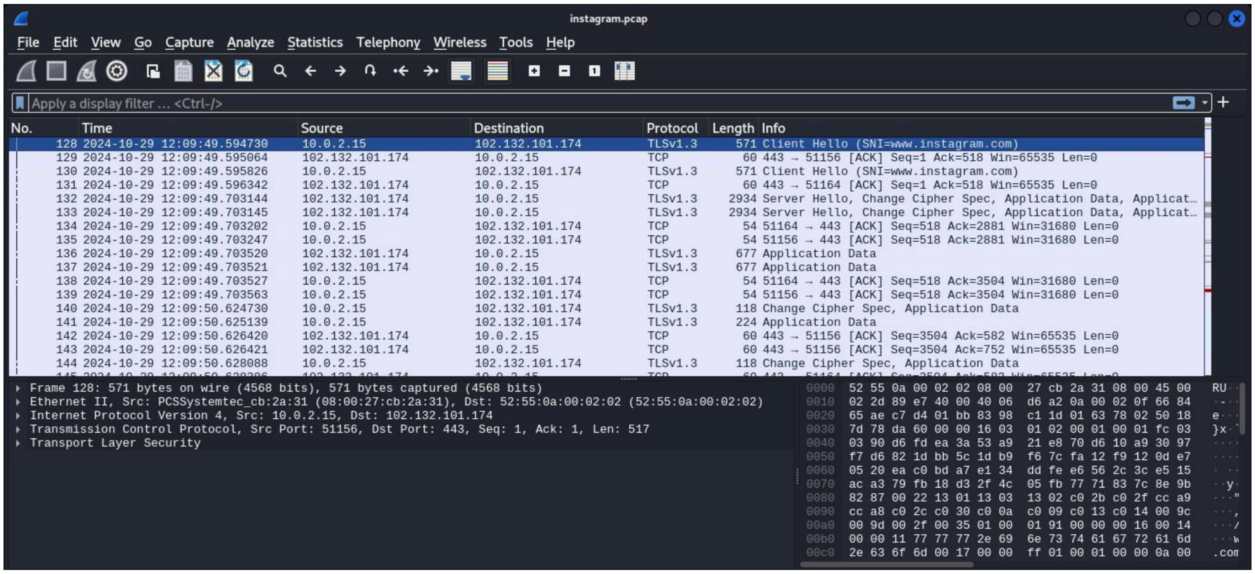
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth0 -nn -s0 -v port 443 -w /home/kali/Desktop/instagram.pcap
[sudo] password for kali:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C2881 packets captured
2881 packets received by filter
0 packets dropped by kernel

┌──(kali㉿kali)-[~]
└─$ 
```

From the image above, tcpdump captured approximately 2881 packets with no packet loss during the access to Instagram.com



The packet file was saved on the desktop as *instagram.pcap*, as specified in the initial command.

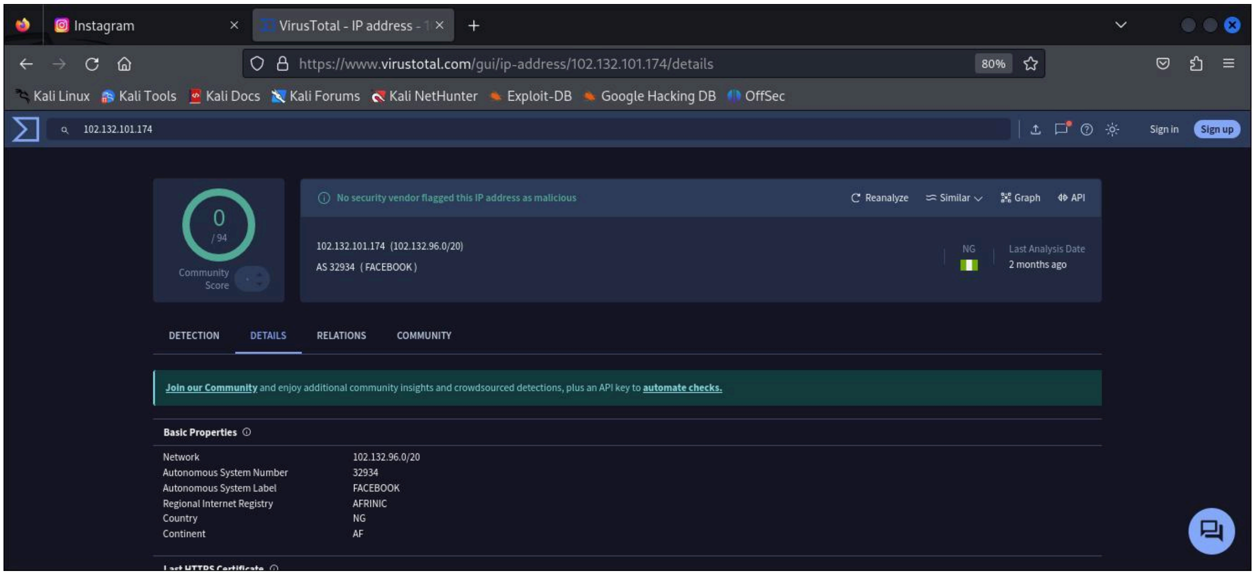

instagram.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time                        Source            Destination       Protocol Length Info
 128 2024-10-29 12:09:49.594730  10.0.2.15         102.132.101.174   TLSv1.3   571 Client Hello (SNI=www.instagram.com)
 129 2024-10-29 12:09:49.595064  102.132.101.174   10.0.2.15         TCP        60 443 → 51156 [ACK] Seq=1 Ack=518 Win=65535 Len=0
 130 2024-10-29 12:09:49.595826  10.0.2.15         102.132.101.174   TLSv1.3   571 Client Hello (SNI=www.instagram.com)
 131 2024-10-29 12:09:49.596342  102.132.101.174   10.0.2.15         TCP        60 443 → 51164 [ACK] Seq=1 Ack=518 Win=65535 Len=0
 132 2024-10-29 12:09:49.703144  102.132.101.174   10.0.2.15         TLSv1.3  2934 Server Hello, Change Cipher Spec, Application Data, Applicat…
 133 2024-10-29 12:09:49.703145  102.132.101.174   10.0.2.15         TLSv1.3  2934 Server Hello, Change Cipher Spec, Application Data, Applicat…
 134 2024-10-29 12:09:49.703202  10.0.2.15         102.132.101.174   TCP        54 51164 → 443 [ACK] Seq=518 Ack=2881 Win=31680 Len=0
 135 2024-10-29 12:09:49.703247  10.0.2.15         102.132.101.174   TCP        54 51156 → 443 [ACK] Seq=518 Ack=2881 Win=31680 Len=0
 136 2024-10-29 12:09:49.703520  102.132.101.174   10.0.2.15         TLSv1.3   677 Application Data
 137 2024-10-29 12:09:49.703521  102.132.101.174   10.0.2.15         TLSv1.3   677 Application Data
 138 2024-10-29 12:09:49.703527  10.0.2.15         102.132.101.174   TCP        54 51164 → 443 [ACK] Seq=518 Ack=3504 Win=31680 Len=0
 139 2024-10-29 12:09:49.703563  10.0.2.15         102.132.101.174   TCP        54 51156 → 443 [ACK] Seq=518 Ack=3504 Win=31680 Len=0
 140 2024-10-29 12:09:50.624730  10.0.2.15         102.132.101.174   TLSv1.3   118 Change Cipher Spec, Application Data
 141 2024-10-29 12:09:50.625139  10.0.2.15         102.132.101.174   TLSv1.3   224 Application Data
 142 2024-10-29 12:09:50.626420  102.132.101.174   10.0.2.15         TCP        60 443 → 51156 [ACK] Seq=3504 Ack=582 Win=65535 Len=0
 143 2024-10-29 12:09:50.626421  102.132.101.174   10.0.2.15         TCP        60 443 → 51156 [ACK] Seq=3504 Ack=752 Win=65535 Len=0
 144 2024-10-29 12:09:50.628088  10.0.2.15         102.132.101.174   TLSv1.3   118 Change Cipher Spec, Application Data
```

```
› Frame 128: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits)
› Ethernet II, Src: PCSSystemtec_cb:2a:31 (08:00:27:cb:2a:31), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 102.132.101.174
› Transmission Control Protocol, Src Port: 51156, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
› Transport Layer Security
```

```
0000  52 55 0a 00 02 02 08 00  27 cb 2a 31 08 00 45 00   RU··
0010  02 2d 89 e7 40 00 40 06  d6 a2 0a 00 02 0f 66 84   ·-··
0020  65 ae c7 d4 01 bb 83 98  c1 1d 01 63 78 02 50 18   e···
0030  7d 78 da 60 00 00 16 03  01 02 00 01 00 01 fc 03   }x·`
0040  03 90 d6 fd ea 3a 53 a9  21 e8 70 d6 10 a9 30 97   ····
0050  f7 d6 82 1d bb 5c 1d b9  f6 7c fa 12 f9 12 0d e7   ····
0060  05 20 ea c0 bd a7 e1 34  dd fe e6 56 2c 3c e5 15   · ··
0070  ac a3 79 fb 18 d3 2f 4c  05 fb 77 71 83 7c 8e 9b   ··y·
0080  82 87 00 22 13 01 13 03  13 02 c0 2b c0 2f cc a9   ···"
0090  cc a8 c0 2c c0 30 c0 0a  c0 09 c0 13 c0 14 00 9c   ···,
00a0  00 9d 00 2f 00 35 01 00  01 91 00 00 00 16 00 14   ···/
00b0  00 00 11 77 77 77 2e 69  6e 73 74 61 67 72 61 6d   ···w
00c0  2e 63 6f 6d 00 17 00 00  ff 01 00 01 00 00 0a 00   .com
```

When viewing the packet file in Wireshark, the details of the queried domain were visible, including the source and destination IPv4 addresses, source and destination ports, etc.



0 / 94
Community Score

No security vendor flagged this IP address as malicious

102.132.101.174 (102.132.96.0/20)
AS 32934 (FACEBOOK)

NG

Last Analysis Date
2 months ago

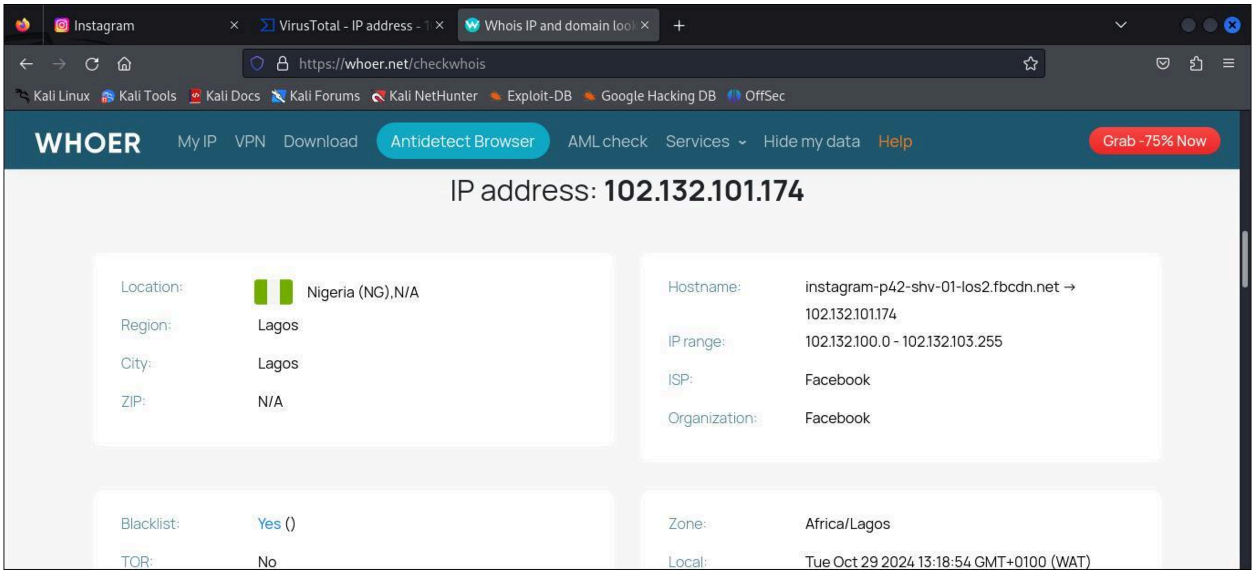
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic Properties

Network	102.132.96.0/20
Autonomous System Number	32934
Autonomous System Label	FACEBOOK
Regional Internet Registry	AFRINIC
Country	NG
Continent	AF

Last HTTPS Certificate

The destination IP address was scanned on VirusTotal.com and found to be safe.



IP address: **102.132.101.174**

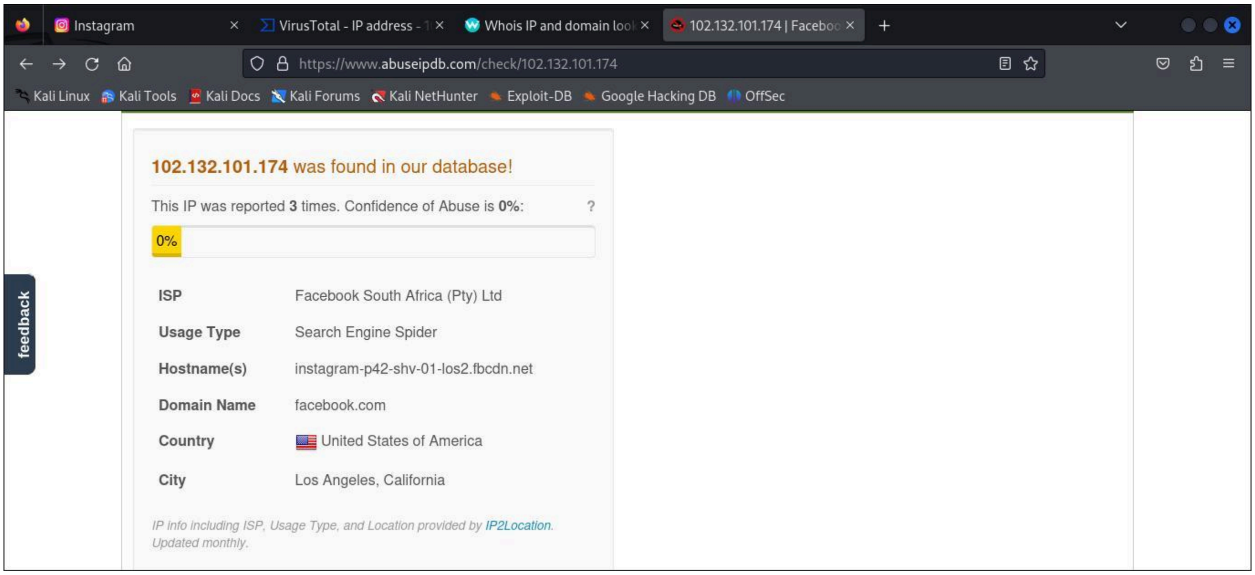
Location:	Nigeria (NG),N/A
Region:	Lagos
City:	Lagos
ZIP:	N/A

Hostname:	instagram-p42-shv-01-los2.fbcdn.net → 102.132.101.174
IP range:	102.132.100.0 - 102.132.103.255
ISP:	Facebook
Organization:	Facebook

Blacklist:	Yes ()
TOR:	No

Zone:	Africa/Lagos
Local:	Tue Oct 29 2024 13:18:54 GMT+0100 (WAT)

A scan of the destination IP address on Whoer.net revealed the ISP, organization, and hostname belongs to Facebook, the company that owns Instagram.



102.132.101.174 was found in our database!

This IP was reported **3** times. Confidence of Abuse is **0%**: ?

0%

ISP	Facebook South Africa (Pty) Ltd
Usage Type	Search Engine Spider
Hostname(s)	instagram-p42-shv-01-los2.fbcdn.net
Domain Name	facebook.com
Country	United States of America
City	Los Angeles, California

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

Further scanning on Abuseipdb showed that the IP has been reported about three times. However, the hostname and domain still confirmed that the IP address belongs to Instagram.

RECOMMENDATION

1. Continue Regular Monitoring: The Instagram security team should maintain continuous network monitoring to detect potential anomalies or threats early, ensuring the network remains secure.

2. Update Security Tools and Databases: All security tools and databases used in the Instagram organization should be updated with the latest versions and malware signatures to stay protected against emerging threats.

3. User Awareness Training: The Instagram security team should regularly train other employees on security best practices and phishing awareness to minimize the likelihood of user-driven security breaches.

CONCLUSION

The analysis and scans did not reveal any signs of malicious activity or suspicious network traffic. All captured packets and IP addresses appear clean and safe based on the tools and databases used (e.g., VirusTotal, AbuseIPDB). Additionally, based on the captured traffic and analysis, the network is currently operating as expected with no indicators of compromise or abnormal behavior.