

# Agenda

- Abstract
- Introduction to Reconnaissance
- Objective of the Project
- Selected Website – Research Details
- Tools Used for Reconnaissance
- Data Collection & Technology Stack
- Impact Analysis
- Recommendations & Mitigation Techniques
- Conclusion
- References

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

# Abstract

- Reconnaissance (Information Gathering) is the first and most crucial phase of cybersecurity assessment. The objective of this project is to study and demonstrate various reconnaissance tools and methods used to collect publicly available information about a target website without directly attacking it.
- In this project, a real website was selected and analyzed using passive and basic active reconnaissance tools such as WHOIS, Nmap, WhatWeb, Wappalyzer, DNS tools, and Google Dorking. The final outcome of this project is a structured understanding of how attackers and security professionals gather information, analyze the technology stack, and assess potential exposure points.
- This report highlights the importance of reconnaissance in cybersecurity, its impact, and recommended mitigation techniques to reduce information leakage.

# Introduction to Reconnaissance

- Reconnaissance is the first phase of cybersecurity assessment.
- It involves gathering publicly available information about a target system, network, or website to identify possible attack vectors.
- Used by ethical hackers to identify weaknesses.
- Also known as Information Gathering, is the first phase of the Cyber Kill Chain.
- Helps understand the attack surface of a website or network.
- Reconnaissance can be:
- Passive Reconnaissance – No direct interaction with the target (safe & legal)
- Active Reconnaissance – Direct interaction with the target (e.g., port scanning)

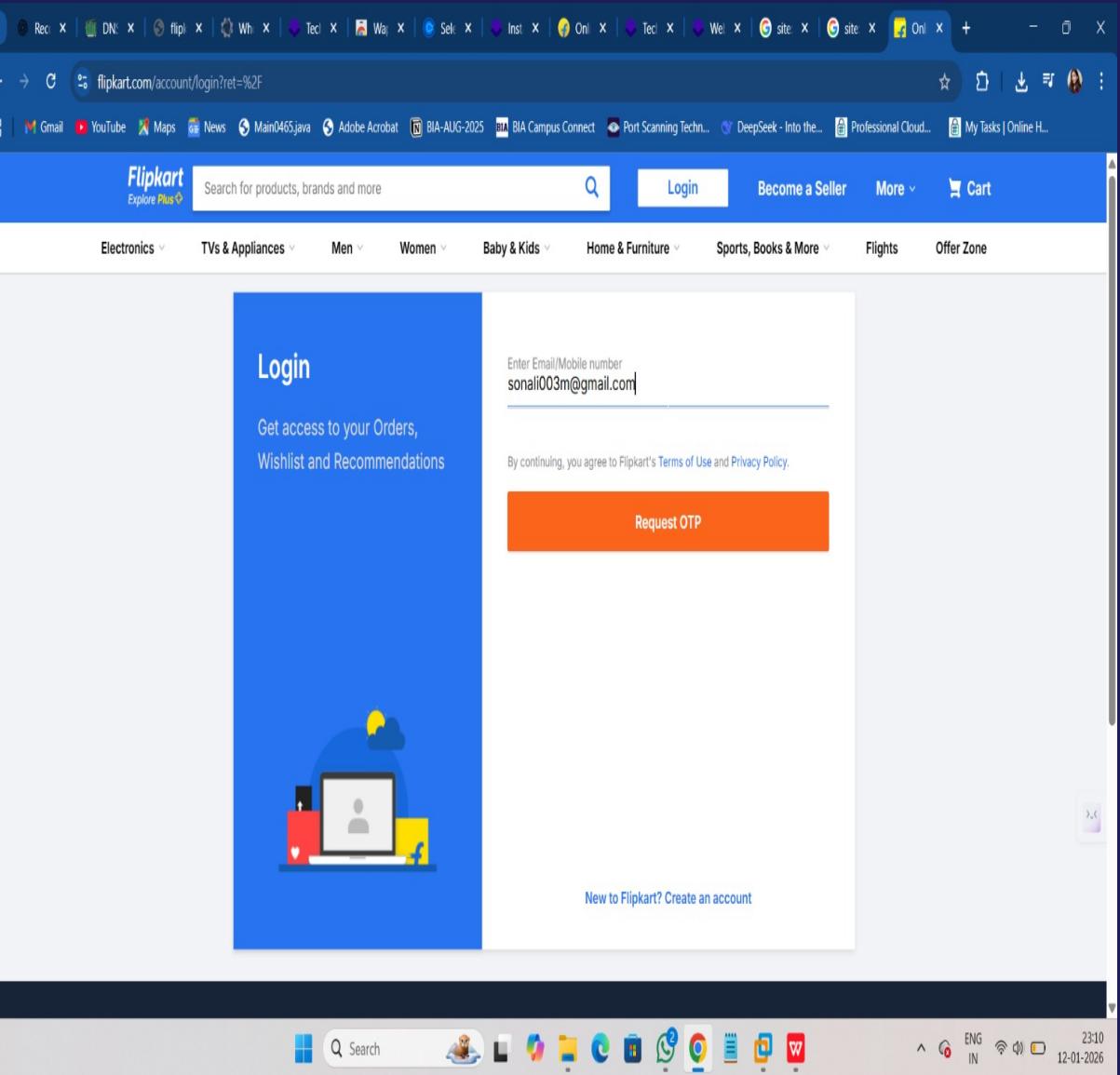
# Objective of the Project

- To understand the role of reconnaissance as the first phase of cybersecurity assessment
- To perform ethical information gathering on a real-world website (Flipkart.com)
- To identify publicly exposed information such as domain details, DNS records, IP addresses, and technologies
- To analyze the technology stack used by Flipkart.com without exploiting vulnerabilities
- To differentiate between passive and active reconnaissance techniques
- To understand how attackers can use gathered information for further attacks
- To highlight the importance of minimizing information leakage
- To gain hands-on experience with reconnaissance tools used in cybersecurity

Note: The following website is used only for educational and passive analysis purposes.

<u>Parameter</u>	<u>Details</u>
Website Name	: Flipkart
URL	: <a href="https://www.flipkart.com">https://www.flipkart.com</a>
Category / Type	: E-Commerce
Business Type	: Online Retail Platform
Popularity / Ranking	: One of India's top e-commerce websites
Users	: Millions of daily active users
Technology Nature	: Large-scale cloud-based platform

# Selected Website – Research Details



The screenshot shows the Flipkart account login interface. A search bar at the top contains the URL "flipkart.com/account/login?ret=%F". Below the header, there are navigation links for Electronics, TVs & Appliances, Men, Women, Baby & Kids, Home & Furniture, Sports, Books & More, Flights, and Offer Zone. The main content area features a blue "Login" form. It includes a placeholder "Enter Email/Mobile number" with the value "sonali003m@gmail.com", a "Request OTP" button, and a note about agreeing to Terms of Use and Privacy Policy. At the bottom right of the form, there is a link "New to Flipkart? Create an account". The status bar at the bottom right shows system information like battery level, signal strength, and the date/time "12-01-2026".

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized use, disclosure, or distribution of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

# Tools Used for Reconnaissance

- WHOIS Lookup
- DNS Enumeration
- Wappalyzer
- WhatWeb
- Nmap
- Google Dorking
- IP Address & Hosting Information
- OSINT via Shodan (Passive)
- THEHARVESTER (OSINT & Email Reconnaissance)
- Robots.txt File Analysis
- HTTP Header Analysis

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

## 1. WHOIS Lookup

### Purpose:

To collect domain ownership and registration details.

- WHOIS privacy protection enabled.

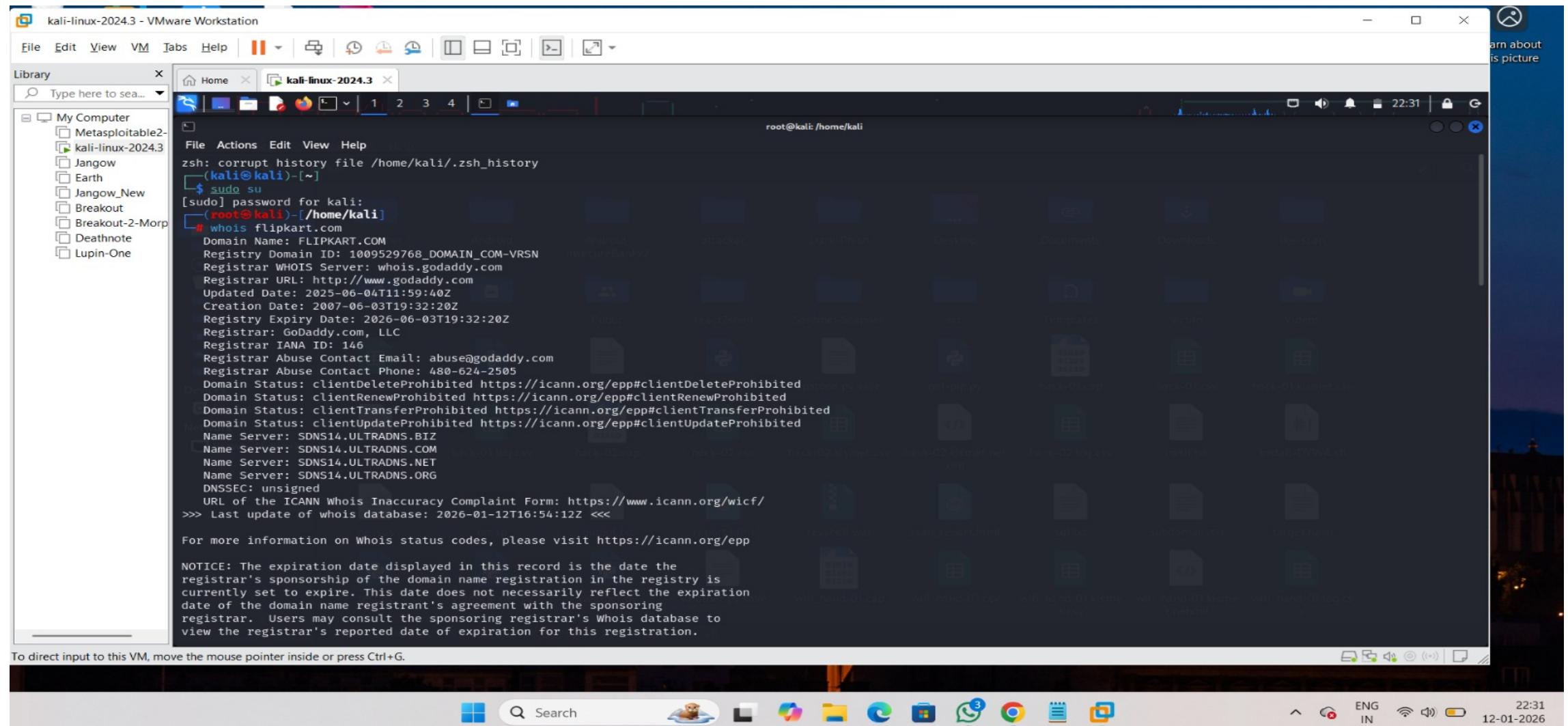
### Information Collected:

- Domain owner
- Registrar and Organization details
- Creation & expiry date
- Name servers

### Outcome:

- Domain ownership information identified.

# WHOIS Lookup - 1



```
File Edit View VM Help
Library Type here to search...
My Computer
Metasploitable2
kali-linux-2024.3
Jangow
Earth
Jangow_New
Breakout
Breakout-2-Morp
Deathnote
Lupin-One

File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
# whois flipkart.com
Domain Name: FLIPKART.COM
Registry Domain ID: 1009529768_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2025-06-04T11:59:40Z
Creation Date: 2007-06-03T19:32:20Z
Registry Expiry Date: 2026-06-03T19:32:20Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: SDNS14.ULTRADNS.BIZ
Name Server: SDNS14.ULTRADNS.COM
Name Server: SDNS14.ULTRADNS.NET
Name Server: SDNS14.ULTRADNS.ORG
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2026-01-12T16:54:12Z <<

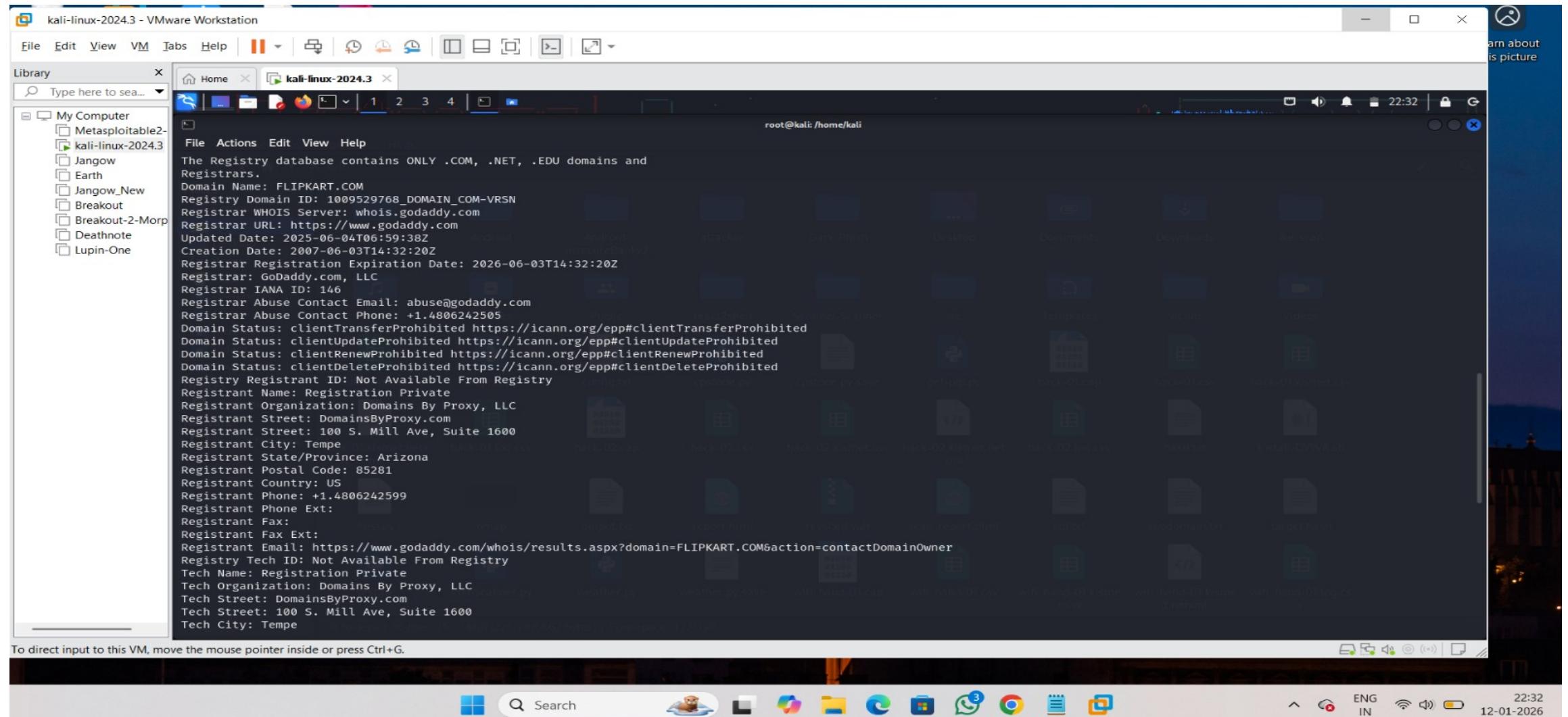
For more information on Whois status codes, please visit https://icann.org/epp

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.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

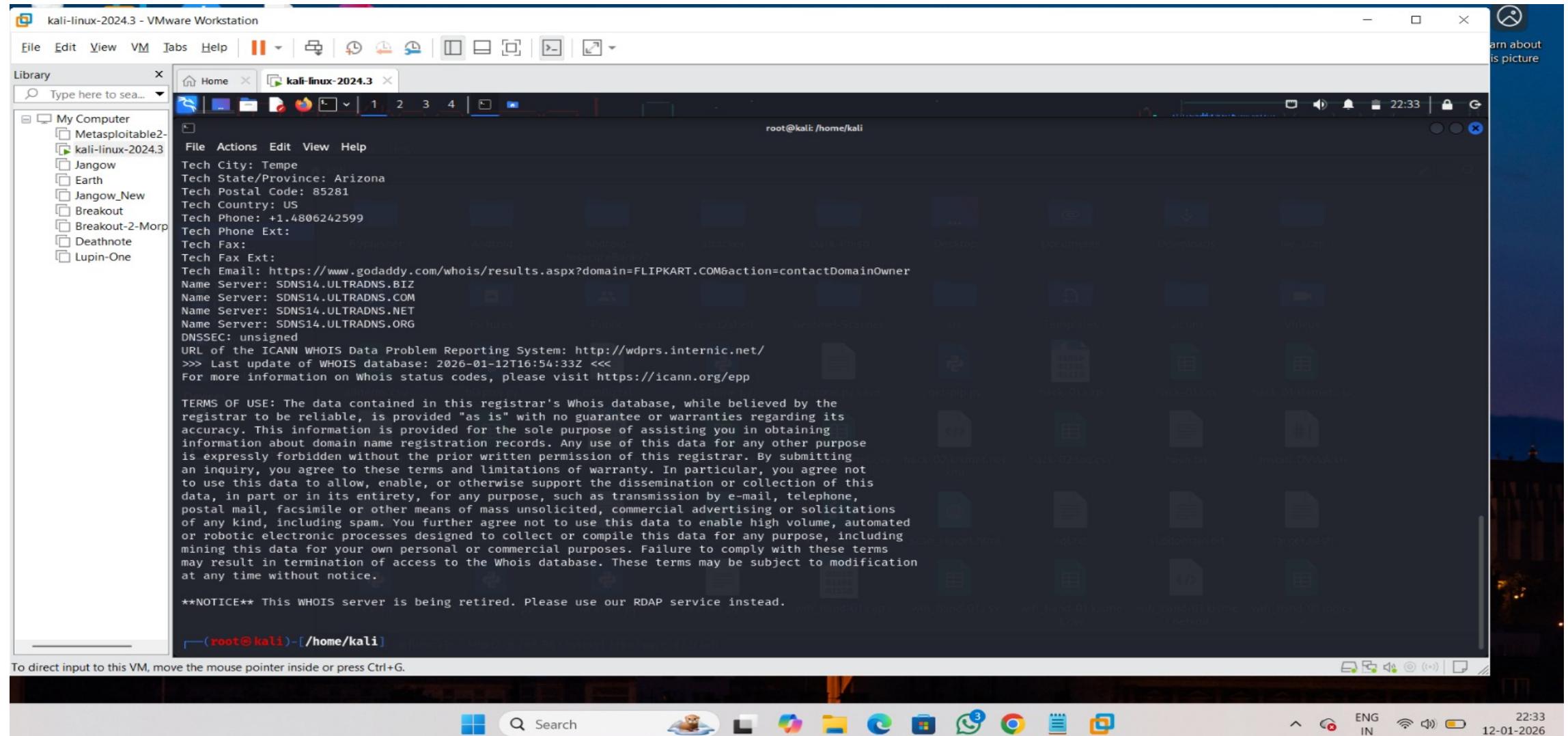
**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

# WHOIS Lookup - 2



**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

## WHOIS Lookup - 3



**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

## 2. DNS Enumeration

### Tool Used:

- DNSDumpster
- nslookup

### Functionality:

- Identifies DNS records (A, MX, NS)
- Finds subdomains

### Outcome:

- Multiple subdomains detected.
- Cloud-based DNS infrastructure observed.

# DNSDumpster - 1

Reconnaissance Tools Report    DNSDumpster - Find & lookup    Whois Lookup, Domain Availability

dnsdumpster.com

Gmail YouTube Maps News Main0465.java Adobe Acrobat BIA-AUG-2025 BIA BIA Campus Connect Port Scanning Techn... DeepSeek - Into the... Professional Cloud... My Tasks | Online H...

Enter a Domain to Test  
flipkart.com

Start Test!

>> Free users are limited to 50 results for a single domain. Get 12 months [Plus Access](#) - on Sale Now.

System Locations

Hosting / Networks

FKNET-IN Flipkar	9
SENDGRID	1
GOOGLE-CLOUD-PLA	1
SECURITYSERVICES	1
MICROSOFT-CORP-M	1

Services / Banners

nginx	9
HTTP/1.1 400 Bad Request	1
istio-envoy	1
nginx/1.14.0 (Ubuntu)	1

Showing 50 records out of a total of 193 found.

Search

ENG IN 22:39 12-01-2026

CONFIDENTIAL: The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

## DNSDumpster - 2

A Records (subdomains from dataset)					
Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
ac.flipkart.com	103.243.33.19	ASN 9752 103.243.33.0/24	FKNET-IN Flipkart Internet Pvt Ltd, IN India		:
accounts.flipkart.com	103.243.32.90	ASN 9752 103.243.32.0/24	FKNET-IN Flipkart Internet Pvt Ltd, IN India	6	:
adfs.flipkart.com	115.114.191.195 in2.mx1.mailhostbox.com	ASN 4755 115.114.191.0/24	TATACOMM-AS TATA Communications formerly VSNL is Leading ISP, IN India	1	:
adp.flipkart.com	103.243.32.24	ASN 9752 103.243.32.0/24	FKNET-IN Flipkart Internet Pvt Ltd, IN India	2	:
ads.flipkart.com	52.172.39.71	ASN 8075 52.160.0.0/11	MICROSOFT-CORP-MSN-AS-BLOCK India	2	:
advertising.flipkart.com	103.243.32.111	ASN 9752 103.243.32.0/24	FKNET-IN Flipkart Internet Pvt Ltd, IN India	1	:
affiliate.flipkart.com	103.243.32.94	ASN 9752 103.243.32.0/24	FKNET-IN Flipkart Internet Pvt Ltd, IN India	1	:
edigateway-prod.api.flipkart.com	163.53.77.16	ASN 9752 163.53.77.0/24	FKNET-IN Flipkart Internet Pvt Ltd, IN India	4	:
1.fdp.api.flipkart.com	103.243.32.9	ASN 9752 103.243.32.0/24	FKNET-IN Flipkart Internet Pvt Ltd, IN India	1	:
2.fdp.api.flipkart.com	163.53.76.115	ASN 9752 163.53.76.0/24	FKNET-IN Flipkart Internet Pvt Ltd, IN India	1	:

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

# DNSDumpster - 3

The screenshot shows a web browser window with three tabs open: "Reconnaissance Tools Report", "DNSDumpster - Find & lookup", and "Whois Lookup, Domain Availability". The main content area is titled "dnsdumpster.com" and shows the following information:

dnsdumpster.com 156.154.142.0/24 United States

TXT Records

```
*MS=ms94028583*
*google-site-verification=NEGXJxq-YmreYBDEfW3NVnz5UAXX7nsekylT68t79fg*
*_globalsign-domain-verification=bUrRwaiTSLb6is-7YeKsgJGyITdbpbKwDuJFqhFmkor*
*MS=ms55469658*
*_globalsign-domain-verification=7UKZuWgB6vmpQnMirigM_TwxalKE6tHsSwoThqtv-K*
*_spf-eemea.onbmc.com*
*H=GwmgnZHJAKGcpRtw@KFTUEH7YLcksjFI7avxc834=
*MS=ms31449763*
*google-site-verification=Y3dKKFu_H3cJ3l660Bt0QIUL3\010Z6cXR0Uxh1Sdc281Y*
*clojars_flipkartoss*
*successFactors-site-verification=YTz10Tg4YzIwOW1MWRnHQ5ZGH00DizNDFhNjF1N0d1YzI0YWW3ZTM5MzFjNDZjMTIwNTJkMTYxYM3NjQ4ZA==
*atlassian-domain-verification=M7Fgf2m5Y3d.8wOH8Q0lsxtTydGU1voasct08IKb1ordbAMkImKsajJHkd6UPrJ*
*successFactors-site-verification=NjQzNDN1YjQ4NnJzZGE30DMyMWIwZTNjNmEwZDlxMnNkNMQSMU3MnY5ZjgxZjYzZTdjZjFKYjB1ZDM3ZGJ1Nw==*
*n6266wQMyPn1LrgMEQ1WTafNmrwQmILR8MZZY6k-
*google-site-verification=qe6w5aA7Jj6U8MPwr3p0bHFEIyn9xL5kBAb5iiaBUQA*
*_globalsign-domain-verification=Q80-agUr5T56L0yznnd3IIloJU0df1C2v2q6duAIE1*
*google-site-verification=a8AROMit-DLHJdmYp1-bq-etV0NlpC5xDCKtHJDYz0*
*onetrust-domain-verification=d61d9ce9635c4528b2a69148684e9a59*
*adobe-idp-site-verification=@0fc98e1-5115-402f-8be0-49c4deadfd56*
*A2326006D53F012A497F*
*_globalsign-domain-verification=1FKrdKwj6jnt7AK_UFbfIMv7KNOWaKRjFapuSUBHG8*
*atlassian-domain-verification=MkV5HFBjxPnPzapALMERVsng8Gy05K60MM5mDdGav02buSbleKNeEvKz0Sa4ld6xGn2*
*v=spf1 include:eu._netblocks.mimecast.com include:zoho.flipkart.com include:_spf.google.com include:spf.protection.outlook.com include:spf.flipkart.com
ip4:64.56.194.128/28 ip4:21 ip4:129.91.5.0/21 ip4:141.145.85.0/24 ip4:1 * "60.34.0.0/16 ip4:199.167.173.0/24 ip4:205.223.80.0/20
ip4:208.72.88.0/21 ip4:216.136.162.64/26 ip4:216.136.168.32/28 ip4:216.136.168.64/27 ip4:216.136.229.0/24 ip4:103.4.255.64/26 ip4:103.4.254.64/26 ip4:103.4.253.64/26
ip6:2405:ba00:8800::/48 ip6:2405:ba * "00:8800::/48 ip6:2606:b400::/32 ip6:2801:1:8800::/48 ip6:2a02:6900:8804::/48 ip6:2a02:6900:8810::/48 ip6:2a02:6900:8814::/48
include:spf.mandrillapp.com ~all*
*_globalsign-domain-verification=139_gF3zeh3avmm9ydAcg3ZXMoJZJP17akkbg10cRj*
*tCrETfqTUKM7U/5AnUIFcFGnFbqfGExd8urSndvq0cQ=
```

At the bottom of the page, there is a "Download .txt" button.

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

## nslookup - 4

The screenshot shows a Kali Linux VM in VMware Workstation. The desktop environment is Unity. Three terminal windows are open, all running as root:

- Terminal 1:** Shows the command `nslookup -type=NS flipkart.com`. It returns non-authoritative answers from four nameservers: `sdns14.ultradns.org.`, `sdns14.ultradns.net.`, `sdns14.ultradns.com.`, and `sdns14.ultradns.biz.`
- Terminal 2:** Shows the command `nslookup -type=MX flipkart.com`. It returns non-authoritative answers from two mail exchangers: `eu-smtp-inbound-2.mimecast.com.` and `eu-smtp-inbound-1.mimecast.com.`
- Terminal 3:** Shows the command `nslookup flipkart.com`. It returns a non-authoritative answer with the name `flipkart.com` and address `103.243.32.90`.

The desktop background features a night cityscape, and the taskbar at the bottom includes icons for various applications like File Explorer, Firefox, and terminal.

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

### 3. Technology Stack Detection – Wappalyzer

#### **Purpose:**

- Identify frontend, backend, server, and security technologies.

#### **Detected Components:**

- Web frameworks
- CDN services
- Analytics tools
- Security mechanisms

# Technology Stack Detection - Wappalyzer - 1

The screenshot shows a Microsoft Edge browser window with the Wappalyzer extension active. The address bar displays 'flipkart.com'. The Wappalyzer interface is overlaid on the right side of the page, listing various technologies detected on the site.

**Detected Technologies:**

- JavaScript frameworks:
  - React
- Reverse proxies:
  - Nginx
- Miscellaneous:
  - Open Graph
- Web servers:
  - Nginx
- Performance:
  - Priority Hints
- JavaScript libraries:
  - React Native for Web
  - Lodash 4.17.21
  - Loadable-Components

**Flipkart Website Content:**

- Header:** Flipkart Explore Plus
- Search Bar:** Search for Products, Brands and More
- Category Links:** Minutes, Mobiles & Tablets, Fashion, Electronics, TVs & Appliances
- Banner:** Akasa Air New Year Up to Book your
- Bottom Banner:** REPUBLIC DAY SALE | Early Bird Deals | EARLY BIRD DEALS LIVE! featuring the Red Fort and two men saluting.

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

## 4. Website Fingerprinting – WhatWeb

### Purpose:

- Fingerprint website technologies

### Command Used:

```
whatweb https://www.flipkart.com
```

### Outcome:

- Server information
- Framework detection
- Security headers identified

# Website Fingerprinting – WhatWeb - 1

The screenshot shows a Kali Linux 2024.3 VM running in VMware Workstation. The terminal window displays the results of a WhatWeb scan against the website <https://www.flipkart.com>. The output includes the following details:

```
(root㉿kali)-[~/home/kali]
# whatweb https://www.flipkart.com

^C/usr/lib/ruby/vendor_ruby/whatweb/scan.rb:75:in `alive?': Interrupt
    from /usr/lib/ruby/vendor_ruby/whatweb/scan.rb:75:in `block (2 levels) in scan'
    from /usr/lib/ruby/vendor_ruby/whatweb/scan.rb:75:in `map'
    from /usr/lib/ruby/vendor_ruby/whatweb/scan.rb:75:in `block in scan'
    from <internal:kernel>:187:in `loop'
    from /usr/lib/ruby/vendor_ruby/whatweb/scan.rb:71:in `scan'
    from /usr/bin/whatweb:619:in `<main>'

(root㉿kali)-[~/home/kali]
# whatweb https://www.flipkart.com

https://www.flipkart.com [200 OK] Cookies[K-ACTION,SN,T,at,ud], Country[INDIA][IN], Email[app-feedback@flipkart.com], HTML[ON,SN,at,ud], IP[103.243.32.90], Open-Graph-Protocol, Script[application/json,application/ld+json], Title[Online Shopping, Furniture, Grocery, Lifestyle, Books & More. Best Offers!], UncommonHeaders[content-security-policy,x-request-id,accept-ch],
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

## 5. Network Scanning - Nmap

### Purpose:

- Identify open ports and services.

### Command Used:

```
nmap -F flipkart.com
```

```
nmap -sV flipkart.com
```

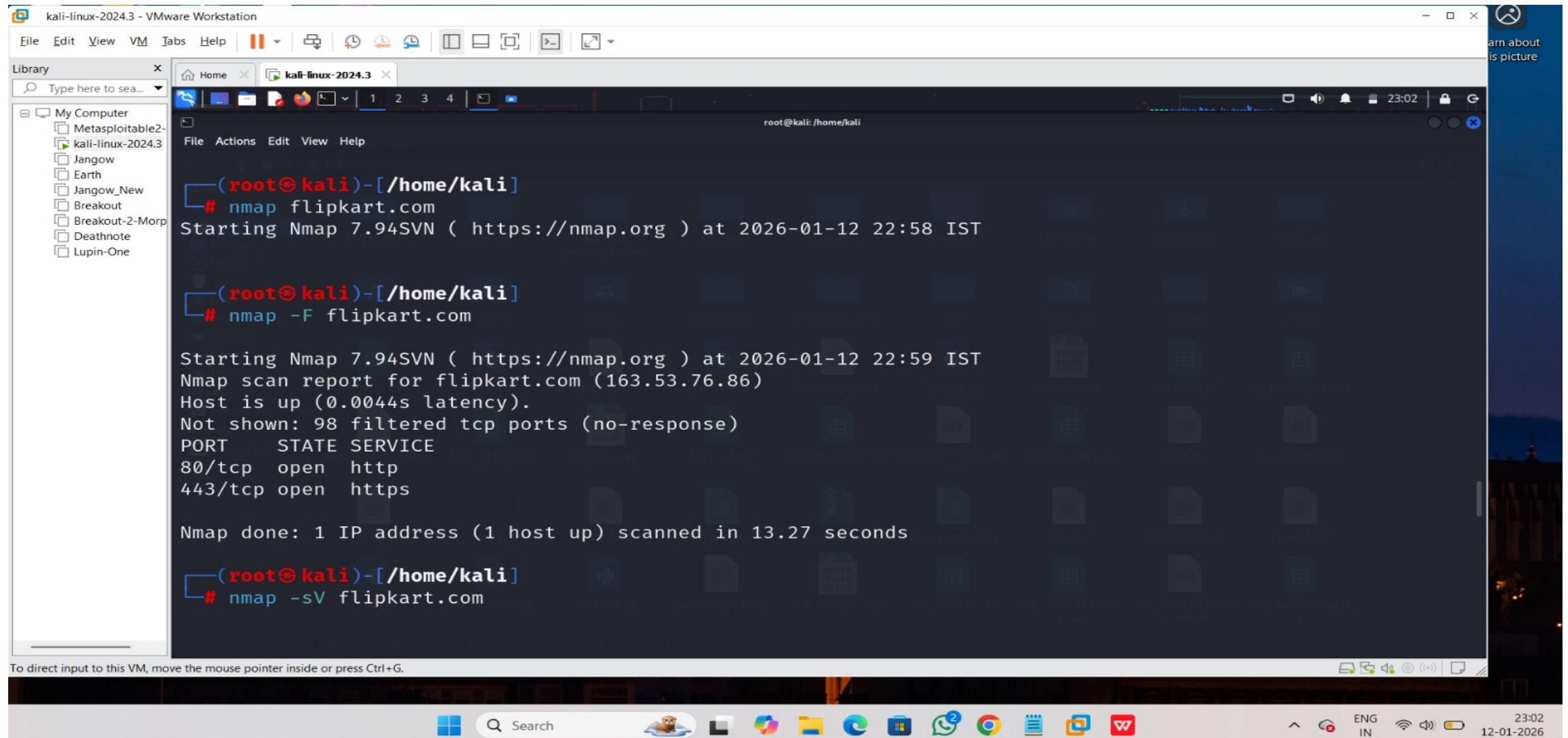
### Functionality:

- Port scanning
- Service enumeration

### Outcome:

- Limited open ports.
- Firewall and security filtering detected.

# Network Scanning - Nmap - 1



The screenshot shows a Kali Linux virtual machine in VMware Workstation. The desktop environment is Unity. Three terminal windows are open, all running under root privilege (root@kali: /home/kali). The first terminal shows the command `# nmap flipkart.com` and its output, which includes the host being up at 163.53.76.86 with ports 80/tcp and 443/tcp open. The second terminal shows the command `# nmap -F flipkart.com` and its output, which is identical to the first scan. The third terminal shows the command `# nmap -sV flipkart.com` and its output, which includes version detection for the open ports.

```
(root@kali)-[/home/kali]
# nmap flipkart.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-12 22:58 IST
Nmap scan report for flipkart.com (163.53.76.86)
Host is up (0.0044s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds

(root@kali)-[/home/kali]
# nmap -F flipkart.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-12 22:59 IST
Nmap scan report for flipkart.com (163.53.76.86)
Host is up (0.0044s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds

(root@kali)-[/home/kali]
# nmap -sV flipkart.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-12 22:59 IST
Nmap scan report for flipkart.com (163.53.76.86)
Host is up (0.0044s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

# Network Scanning - Nmap - 2

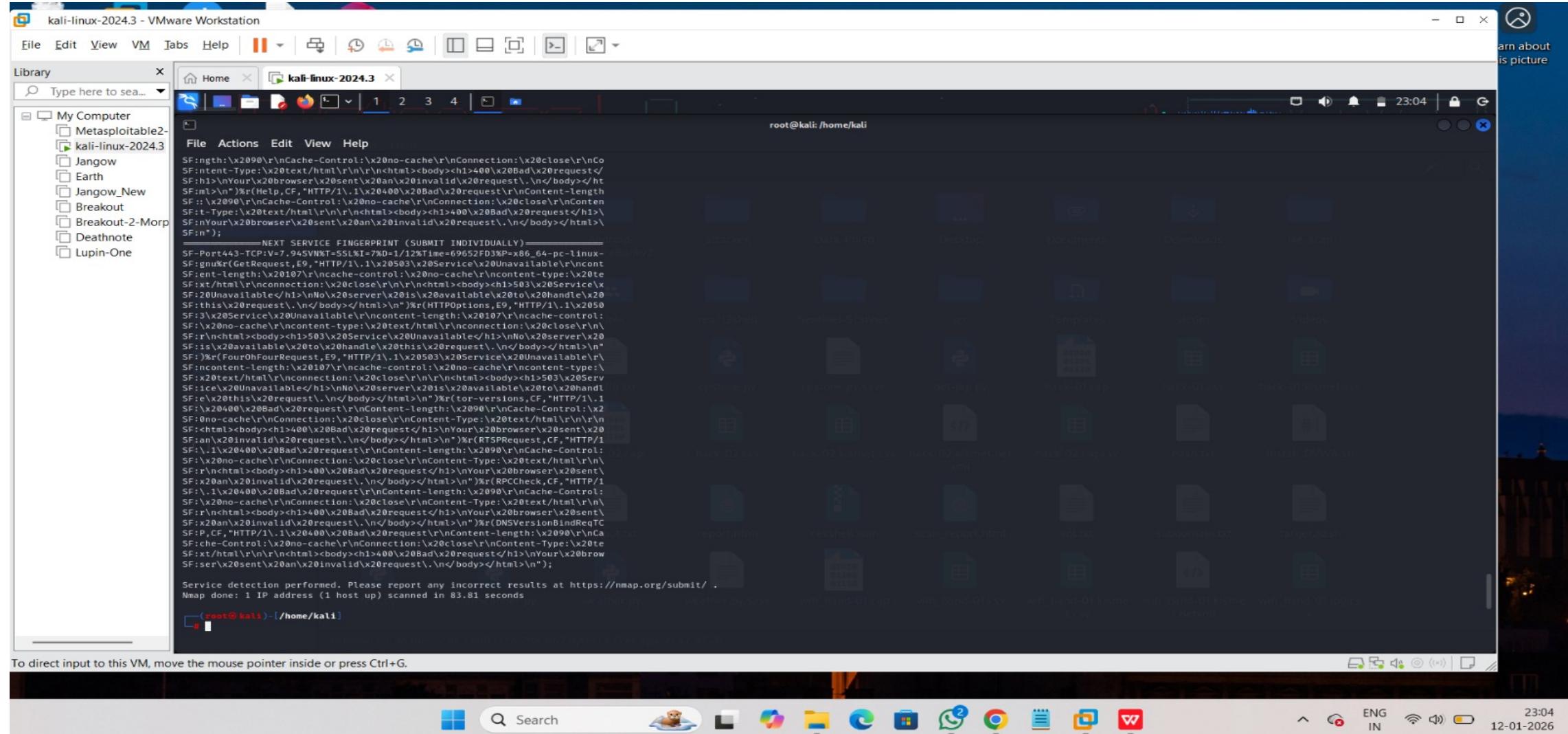
The screenshot shows a Kali Linux 2024.3 VM running in VMware Workstation. The terminal window displays the output of an Nmap scan against the target IP 163.53.76.86. The scan results show several open ports, including port 80 (HTTP) and port 443 (SSL/TLS). The terminal also shows a message from Nmap asking for service fingerprints.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-12 22:59 IST
Nmap scan report for flipkart.com (163.53.76.86)
Host is up (0.093s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http
443/tcp   open  ssl/https nginx
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints
at https://nmap.org/cgi-bin/submit.cgi?new-service :
    NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY) =
SF-Port80-TCP:V=7.94SNSEI=7%D=1/12%Time=69652FCDFP=x86_64-pc-linux-gnu$R(G
SF:etRequest,61,"HTTP/1.1\x20301\x20Moved\x20Permanently\r\nContent-length
SF:h\x200\r\nlocation:\x20https://:43/\r\nconnection:\x20close\r\nr
SF:k(HTTPOptions,61,"HTTP/1.1\x20301\x20Moved\x20Permanently\r\nContent-
SF:length:\x200\r\nlocation:\x20https://:43/\r\nconnection:\x20close\r\nr
SF:r(HTTSPRequest,CF,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-l
SF:ength:x2090\r\nCache-Control:\x20no-cache\r\nConnection:\x20close\r\nC
SF:ontent-Type:\x20text/html\r\nContent-Type:\x20text/html\r\nbody>h1>400\x20Bad\x20Request<
SF:/h1>\nYour browser\x20sent\x20an\x20invalid\x20request.\n</body></h
SF:tml>\n")$r(X11Probe,CF,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-l
SF:ength:x2090\r\nCache-Control:\x20no-cache\r\nConnection:\x20close\r\nC
SF:ontent-Type:\x20text/html\r\nContent-Type:\x20text/html\r\nbody>h1>400\x20Bad\x20Request<
SF:/h1>\nYour browser\x20sent\x20an\x20invalid\x20request.\n</body></h
SF:tml>\n")$r(FourOhFourRequest,84,"HTTP/1.1\x20301\x20Moved\x20Permanent
SF:ly\r\nContent-length:\x200\r\nlocation:\x20https://:443/nice20ports%2C
SF:tr%6Eity,.txt2ebak\r\nconnection:\x20close\r\nr\n")$r(RPCCheck,CF,
SF:HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-length:\x2090\r\nCache-Co
SF:ntrol:\x20no-cache\r\nConnection:\x20close\r\nContent-Type:\x20text/htm
SF:t\r\n\r\n<html><body><h1>400\x20Bad\x20Request</h1>\nYour browser\x2
SF:sent\x20an\x20invalid\x20request.\n</body></html>\n")$r(DNSVersionBin
SF:dReqTCP,CF,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-length:\x2090
SF:\r\nCache-Control:\x20no-cache\r\nConnection:\x20close\r\nContent-Type:
SF:x20text/html\r\nContent-Type:\x20text/html\r\nbody>h1>400\x20Bad\x20Request<
SF:/h1>\nYour browser\x20sent\x20an\x20invalid\x20request.\n</body></h
SF:tml>\n")$r(Helper,CF,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-length
SF::\x2090\r\nCache-Control:\x20no-cache\r\nConnection:\x20close\r\nContent-
SF:t-Type:\x20text/html\r\nContent-Type:\x20text/html\r\nbody>h1>400\x20Bad\x20Request<
SF:/h1>\nYour browser\x20sent\x20an\x20invalid\x20request.\n</body></h
SF:ml>\n");
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

# **Network Scanning - Nmap - 3**



**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

## 6. Google Dorking

### Purpose:

- Extract publicly exposed information

### Examples:

site:flipkart.com

site:flipkart.com filetype:pdf

site:flipkart.com login

site:flipkart.com "@flipkart.com"

### Outcome:

- Public documents identified.
- Support pages.
- No sensitive data exposure found.

# Google Dorking - 1

The screenshot shows a Google search results page with the query "site:flipkart.com" entered in the search bar. The results are as follows:

- Flipkart Brand Assurance**  
https://brandhub.flipkart.com  
Your brand needs more than just protection — it needs the ability to grow. With the new Growth Analytics, you can achieve smarter and faster business growth ... [Read more](#)
- Flipkart Venture Capital**  
https://ventures.flipkart.com  
Flipkart Ventures, the investment arm of Flipkart, is a \$100 million fund founded on a vision to back early-stage startups in India and thereby help support the ... [Read more](#)
- Flipkart Seller Hub: Become an Online Seller in India**  
Create your Flipkart seller account in under 10 minutes with just 1 product and a valid GSTIN number. [Read more](#)
- Flipkart Tech Blog**  
https://tech.flipkart.com

At the bottom of the screen, the Windows taskbar is visible with various pinned icons and the system tray showing the date and time.

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

# Google Dorking - 2

The screenshot shows a Google search results page with the query "site:flipkart.com filetype:pdf". The results are as follows:

- Approved - FlipTrends 2025**  
https://stories.flipkart.com › approved-fliptrends-2... PDF  
17 Dec 2025 — India searched for everything on Flipkart from Labubu to Stanley Cups, proving that. 2025 was the year niche obsessions went national. [Read more](#)
- Flipkart partners with Aegon Life Insurance to offer paperless ...**  
https://stories.flipkart.com › flipkartaegon PDF  
Bengaluru - March 16, 2020: Flipkart, India's homegrown e-commerce marketplace and. Aegon Life Insurance, pioneer of digital insurance in India, ... [Read more](#)
- Flipkart hosts #Include, a product and tech conference ...**  
https://stories.flipkart.com › flipkartpartnerswithw... PDF  
Bengaluru - November 23, 2019: Flipkart, India's leading e-commerce marketplace today organised a conference on building innovative solutions for the ... [Read more](#)
- Press release Flipkart Wholesale launches digital platform in ...**  
Patna - July 5, 2021 · Flipkart Wholesale, the digital B2B marketplace of India's homegrown Elinkart

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

# Google Dorking - 3

The screenshot shows a Google search results page with the query "site:flipkart.com login". The results are as follows:

- Flipkart**  
https://www.flipkart.com › login  
[Login](#)  
No information is available for this page.  
[Learn why](#)
- Flipkart**  
https://www.flipkart.com :  
[Online Shopping Site for Mobiles, Electronics, Furniture ...](#)  
India's biggest online store for Mobiles, Fashion (Clothes/Shoes), Electronics, Home Appliances, Books, Home, Furniture, Grocery, Jewelry, Sporting goods, ...
- Flipkart**  
https://accounts.flipkart.com › ... :  
[Login with Flipkart](#)  
Log in with a CEMP account. Phone number / Email Id. Cemp will get access to your basic profile. By continuing, you agree to our Terms of Use and Privacy ... [Read more](#)
- Flipkart**  
https://www.flipkart.com › internet-login-password-book :  
[Internet Login And Password Book](#)  
Internet Login And Password Book by Frost Sharon from Flipkart.com. Only Genuine Products. 30

At the bottom, the taskbar shows various pinned applications: DNS, flipkart, Whois, Tech, Selena, Insta, Online, Tech, Web, Google site, Google site, and Google site. The system tray indicates ENG IN, 23:09, and 12-01-2026.

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

# Google Dorking - 4

site:flipkart.com "@flipkart.com"

**Buy Flipkart Online at Best Prices In India**  
Flipkart - Shop Flipkart at India's Best Online Shopping Store. Check Price and Buy Online. ✓ Free Shipping ✓ Cash on Delivery ✓ Best Offers.  
4.0 ★ store rating (1.4K)

**24x7 Customer Support**  
I want help with new GST changes ; I want to manage my order. View, cancel or return an order ; I want help with returns & refunds. Manage and track returns ; I ... [Read more](#)

**Dresses - Buy Dresses Online at Best Prices In India**  
Dresses - Shop Dresses at India's Best Online Shopping Store. Check Price and Buy Online. ✓ Free Shipping ✓ Cash on Delivery ✓ Best Offers.

**Flight bookings, Cheap flights, Lowest Air tickets ...**  
Flights Online Store in India. Check Flights Prices, Ratings & Reviews at [Flipkart.com](#). ✓ Free Shipping ✓ Cash on Delivery ✓ Best Offers - Book Cheap flight ...

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

## 7. IP Address & Hosting Information

### Purpose:

- Check if the host is reachable
- Identify approximate IP address

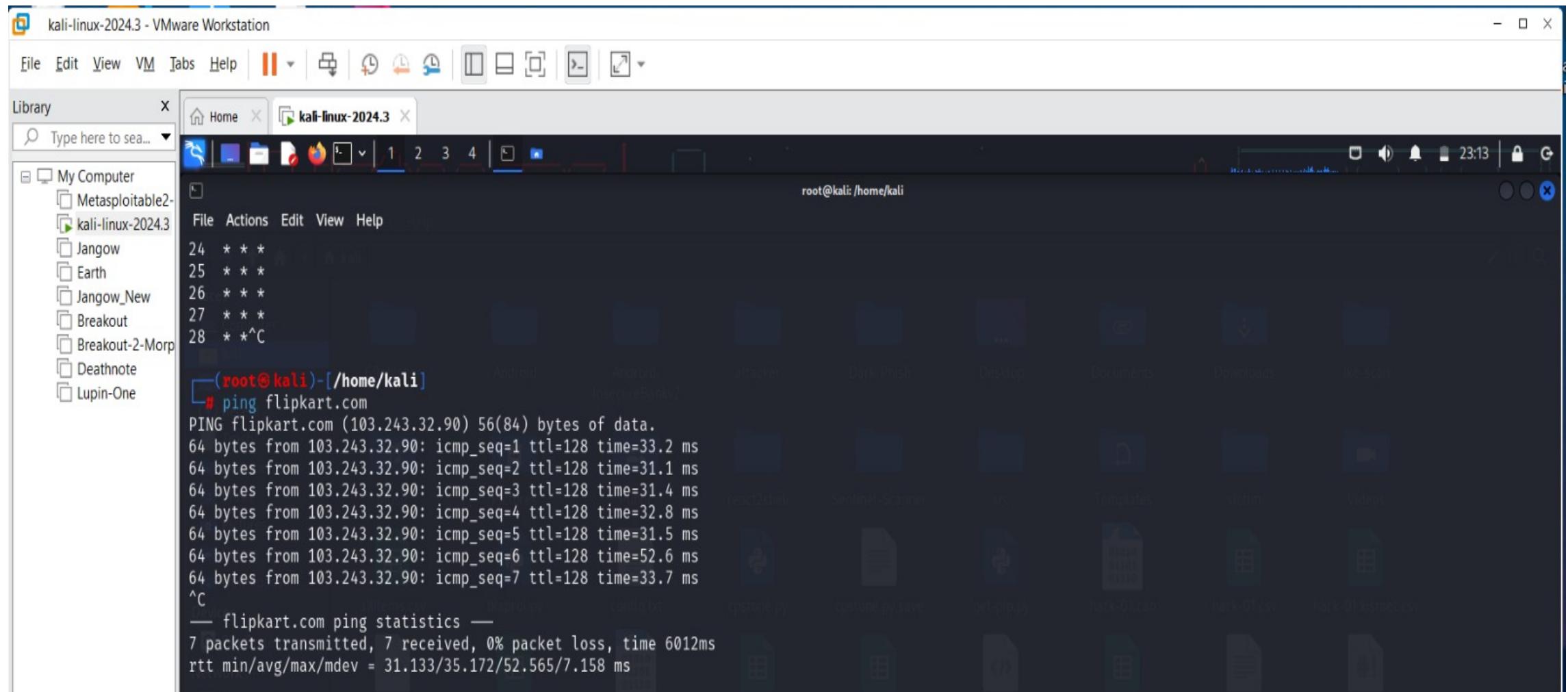
### Command:

```
ping flipkart.com
```

### Outcome:

- Shows response time
- Confirms CDN or load balancer usage

# IP Address & Hosting Information - 1



kali-linux-2024.3 - VMware Workstation

File Edit View VM Tabs Help | || [ ] [ ] [ ] [ ] [ ] [ ]

Library X

Type here to search... ▾

My Computer

- Metasploitable2-...
- kali-linux-2024.3
- Jangow
- Earth
- Jangow\_New
- Breakout
- Breakout-2-Morp...
- Deathnote
- Lupin-One

Home kali

root@kali: /home/kali

```
24 * * *
25 * * *
26 * * *
27 * * *
28 * * ^C

[root@kali]# ping flipkart.com
PING flipkart.com (103.243.32.90) 56(84) bytes of data.
64 bytes from 103.243.32.90: icmp_seq=1 ttl=128 time=33.2 ms
64 bytes from 103.243.32.90: icmp_seq=2 ttl=128 time=31.1 ms
64 bytes from 103.243.32.90: icmp_seq=3 ttl=128 time=31.4 ms
64 bytes from 103.243.32.90: icmp_seq=4 ttl=128 time=32.8 ms
64 bytes from 103.243.32.90: icmp_seq=5 ttl=128 time=31.5 ms
64 bytes from 103.243.32.90: icmp_seq=6 ttl=128 time=52.6 ms
64 bytes from 103.243.32.90: icmp_seq=7 ttl=128 time=33.7 ms
^C
— flipkart.com ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6012ms
rtt min/avg/max/mdev = 31.133/35.172/52.565/7.158 ms
```

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

## 8. OSINT via Shodan (Passive)

### Purpose:

- Identify exposed services

### Method:

- Visit: <https://www.shodan.io>

### Search:

flipkart.com

### Outcome:

- Cloud infrastructure visibility

# OSINT via Shodan (Passive) - 1

Reconn flip DNSDU flipkart Whois Techno Wappa Select Installa Online Techno Website site:flip site:flip Online +

shodan.io/search?query=flipkart.com

Gmail YouTube Maps News Main0465.java Adobe Acrobat BIA-AUG-2025 BIA BIA Campus Connect Port Scanning Techn... DeepSeek - Into the... Professional Cloud... My Tasks | Online H...

Shodan Maps Images Monitor Developer More...

SHODAN Explore Pricing flipkart.com  Login

TOTAL RESULTS 17

TOP COUNTRIES



Country	Count
India	16
United States	1

TOP PORTS

Port	Count
443	11
80	5
53	1

TOP ORGANIZATIONS

Organization	Count
Flipkart Internet Pvt Ltd	15
Google LLC	1
Internet Service Provider	1

 View Report  View on Map  Advanced Search

**Product Spotlight:** Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

**Sell Online on Flipkart | Grow your business with the leader in Indian e-commerce**

SSL Certificate

HTTP/1.1 200 OK  
server: nginx  
date: Mon, 12 Jan 2026 16:57:12 GMT  
content-type: text/html; charset=utf-8  
content-length: 4983  
x-frame-options: SAMEORIGIN  
cache-control: private, no-cache, no-store, must-revalidate  
expires: -1  
pragma: no-cache  
Set-Cookie: T=SD.b6eeda20-4242-4de7-86ed-75c3...

Issued By:  
- Common Name: GlobalSign RSA OV SSL CA 2018

Issued To:  
- Common Name: www.seller.flipkart.com  
- Organization: FLIPKART INTERNET PRIVATE LIMITED

Supported SSL Versions:  
TLSv1.2

SSL Certificate

HTTP/1.1 302 Found  
server: nginx  
date: Mon, 12 Jan 2026 16:54:20 GMT  
content-type: text/html; charset=utf-8  
content-length: 372  
Set-Cookie: nonce=ss-820025574; Max-Age=13434242; Path=/; Expires=Wed, 17 Jun 2026 04:38:22 GMT; HttpOnly  
Set-Cookie: \_csrf=cXSiKPm\_mBQqe4pBRr1d\_tyU; Path=/

Set-C...

2026-01-12T16:57:12.990829 2026-01-12T16:54:20.402597

ENG IN 23:23 12-01-2026

CONFIDENTIAL: The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

## OSINT via Shodan (Passive) - 2

shodan.io/search?query=flipkart.com

SSL Certificate

Issued By:  
- Common Name: GlobalSign RSA OV SSL CA 2018

Issued To:  
- Common Name: www.ads.cloud.flipkart.com  
- Organization: FLIPKART INTERNET PRIVATE LIMITED

Supported SSL Versions:  
TLSv1.2

SSL Certificate

Issued By:  
- Common Name: GlobalSign RSA OV SSL CA 2018

Issued To:  
- Common Name: www.partner.flipkart.com  
- Organization: FLIPKART INTERNET PRIVATE LIMITED

Supported SSL Versions:  
TLSv1.2

Flipkart Ads

CONFIDENTIAL: The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

## OSINT via Shodan (Passive) - 3

The screenshot shows a web browser window with the URL [shodan.io/search?query=flipkart.com](https://shodan.io/search?query=flipkart.com). The results page displays two entries:

**Ekart Logistics** (IP: 163.53.76.136)

**SSL Certificate**  
Issued By: GlobalSign RSA OV SSL CA 2018  
Issued To: www.flipkartrobotics.com  
Supported SSL Versions: TLSv1.2

**HTTP/1.1 200 OK**  
Set-Cookie: empid=; Path=/; Secure; HTTPOnly  
cache-control: max-age=2592000  
x-xss-protection: 1; mode=block  
x-content-type-options: nosniff  
content-security-policy: style-src 'self' 'unsafe-inline' https://flipkartads.azureedge.net https://fonts.googleapis.com/ http

**Flipkart Ads Platform** (IP: 163.53.76.178)

**SSL Certificate**  
Issued By: GlobalSign RSA OV SSL CA 2018  
Issued To: www.brandmanager.flipkart.com  
Supported SSL Versions: TLSv1.2

**HTTP/1.1 200 OK**  
server: nginx  
date: Mon, 12 Jan 2026 15:03:22 GMT  
content-type: text/html; charset=utf-8  
content-length: 101022  
Set-Cookie: nonce=ss-2878962080; Max-Age=13434242; Path=/; Expires=Wed, 17 Jun 2026 02:47:25 GMT; HttpOnly  
Set-Cookie: DID=cmkbalwat0g2d0q3ez4qz7rg9; Max-Age=31556...

The browser interface includes a navigation bar with tabs like Recon, DNSD, flip, Whois, Techno, Wappa, Select, Installa, Online, Techno, Website, site:flip, site:flip, Online, and a search bar. The bottom of the screen shows the Windows taskbar with icons for Search, Start, File Explorer, Task View, and various pinned applications.

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

## 9. THEHARVESTER (OSINT & Email Reconnaissance)

### Purpose:

- Expands OSINT coverage

### Command:

```
theHarvester -d flipkart.com -b bing,duckduckgo,yahoo
```

### Outcome:

- More subdomains
- Additional hosts

**THEHARVESTER (OSINT & Email Reconnaissance) - 1**

The screenshot shows a Kali Linux 2024.3 virtual machine running in VMware Workstation. The terminal window displays the output of theHarvester, a tool for performing OSINT (Open-Source Intelligence) tasks. The command run was `theHarvester -d flipkart.com -b bing,duckduckgo,yahoo`. The output includes details about proxies, API keys, and various hostnames found for the target domain. In the background, a Firefox browser window is open, showing a search results page for "flipkart.com". The taskbar at the bottom of the screen lists several icons, including Skyscanner, 10.10.10.245, localhost, bra-hackers, chatopt, 192.168.32.1, github, and flipkart.

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

## 10. Robots.txt File Analysis

### Purpose:

- To identify directories and URLs restricted from search engine indexing
- Helps understand which sections of the website are intentionally hidden from crawlers

### Command:

```
curl https://www.flipkart.com/robots.txt
```

### Outcome:

- Displays a list of disallowed paths for search engines
- Indicates areas that are not indexed publicly
- Useful for understanding information exposure control

# Robots.txt File Analysis - 1

The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. The main focus is a Firefox browser window displaying the robots.txt file for the website <https://www.flipkart.com/robots.txt>. The browser's address bar and tabs are visible at the top. On the left, a file manager window titled "kali-linux-2024.3" shows the contents of the "My Computer" drive, including various Kali Linux and Metasploitable virtual machines. The Firefox window contains the following content:

```
User-agent: Mediapartners-Google
Disallow:

User-agent: Adsbot-Google
Disallow:

User-agent: Googlebot-Image
Disallow:

# cart
User-agent: *
Disallow: /viewcart

# Something related to carousel and recommendation carousel
User-agent: *
Disallow: /dynamic/

# Permanent Link For Individual Review
User-agent: *
Disallow: /reviews/

# Old Browse Page Experience
User-agent: *
Disallow: /store/

# Affiliate Widget
User-agent: *
Disallow: /affiliateWidget/

# Social Connect Redirects
User-agent: *
Disallow: /sc/

# Product Seller Pages
User-agent: *
Disallow: /ps/

# Temporary Hack
User-agent: *
Disallow: /ph/search/

#Alliances Pages
User-agent: *
Disallow: /alliances/
```

At the bottom of the browser window, there is a message: "To direct input to this VM, move the mouse pointer inside or press Ctrl+G." The system tray at the bottom right shows various icons and the date/time: 23:26, 12-01-2026.

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

# Robots.txt File Analysis - 2

The image shows two side-by-side screenshots of a Kali Linux VM running in VMware Workstation. Both screenshots display the contents of the `flipkart.com/robots.txt` file in a web browser tab.

**Left Screenshot:** Shows the initial portion of the robots.txt file, which includes rules for various user-agents and sections like `# Post Order Pages` and `# AMP Pages`.

```
user-agent: *
Disallow: /*?colorSelected=
Disallow: /*?layout=
Disallow: /*?primarySection=
Disallow: /*?sizeSelected=
Disallow: /*&colorSelected=
Disallow: /*&layout=
Disallow: /*&primarySection=
Disallow: /*&sizeSelected=
Disallow: *facets*
Disallow: *sort*
Disallow: */-cs-
Disallow: /*/easysize*
Disallow: /*3/product/*
Disallow: /*answers/*
Disallow: /*immerse?*
Disallow: /*item/product-delivery*
Disallow: /*item/product-warranty*
Disallow: /*item/seller-callout/itemId?*
Disallow: /*login?*
Disallow: /*offer-details*
Disallow: /*payments-callout/*
Disallow: /*pbo-offer*
Disallow: /*pp-protect-promise-fee?*
Disallow: /*pp/*
Disallow: /*product-emi-details?*
Disallow: /*product-questions?*
Disallow: /*products-list/bought-together?*
Disallow: /*products-list/recommended-for-you?*
Disallow: /*quick-view?*
Disallow: /*review-image-fullscreen?*
Disallow: /*review-image-grid?*
Disallow: /*review-video-fullscreen*
Disallow: /*review-video-grid*
Disallow: /*review-media-grid*
Disallow: /*rpd-product-details?*
Disallow: /*rv/sizechart?*
Disallow: /*seller-details?*
Disallow: /*sellers?*
Disallow: /*specifications?*
Disallow: /*swatch?*
Disallow: /*threed-main-compare-view?*
Disallow: /*user-address?*
Disallow: /*video-player?*
```

**Right Screenshot:** Shows the continuation of the robots.txt file, specifically the `Sitemap` section which lists numerous URLs for product sitemaps.

```
Sitemap: https://www.flipkart.com/sitemap_v_view-browse.xml.gz
Sitemap: https://www.flipkart.com/sitemap_p_product_index_1.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_2.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_3.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_4.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_5.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_6.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_7.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_8.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_9.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_10.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_11.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_12.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_13.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_14.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_15.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_16.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_17.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_18.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_19.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_20.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_21.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_22.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_23.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_24.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_25.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_26.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_27.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_28.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_29.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_30.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_31.xml
Sitemap: https://www.flipkart.com/sitemap_p_product_index_32.xml
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

## 11. HTTP Header Analysis

### Purpose:

- View HTTP response headers

### Command:

```
curl -I https://www.flipkart.com
```

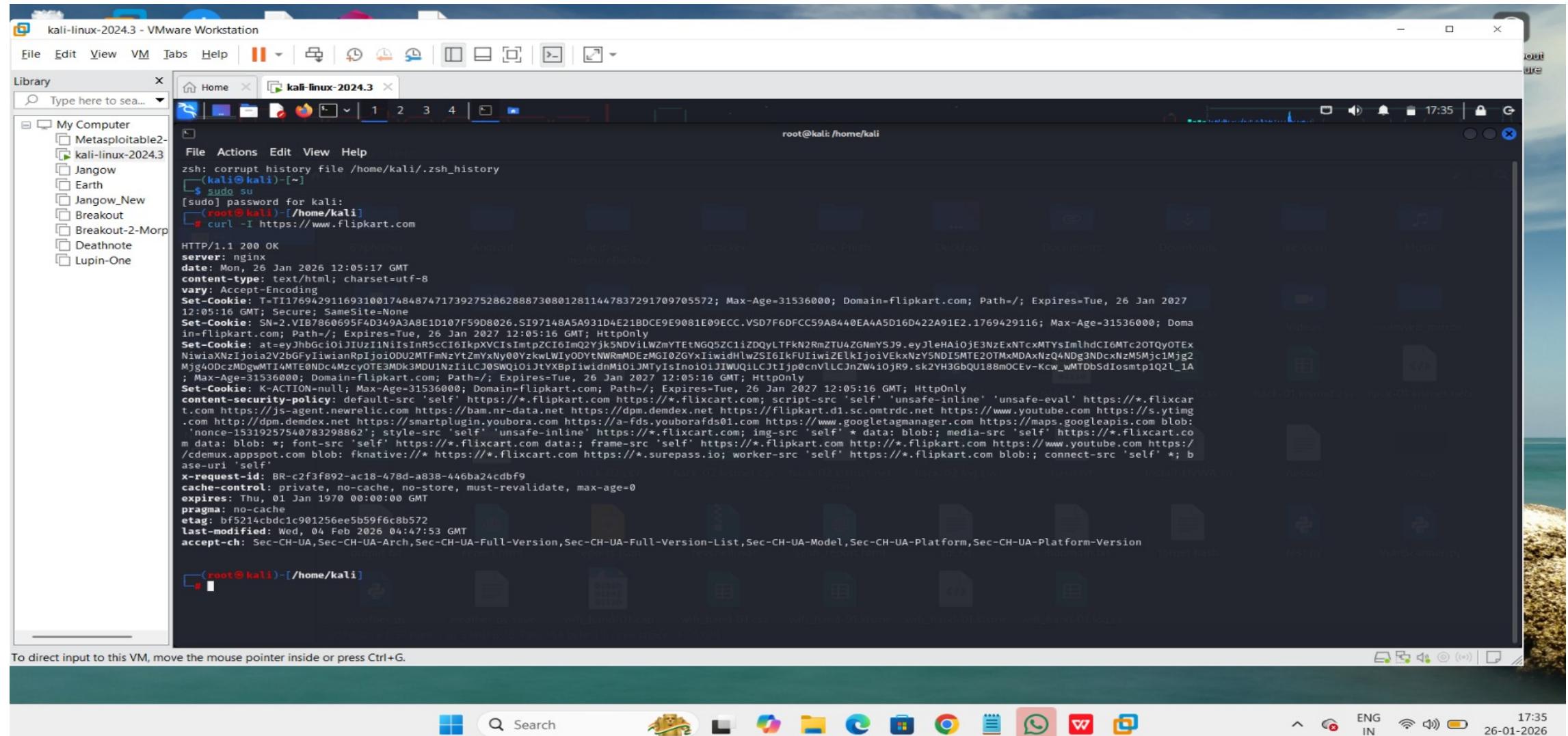
### Information Collected:

- Server type
- Security headers
- Cookies

### Outcome:

- Confirms HTTPS
- Security policies detected

# HTTP Header Analysis - 1



The screenshot shows a Kali Linux terminal window titled "kali-linux-2024.3 - VMware Workstation". The terminal displays the following command and its output:

```
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
[root@kali] ~
# curl -I https://www.flipkart.com
HTTP/1.1 200 OK
server: nginx
date: Mon, 26 Jan 2026 12:05:17 GMT
content-type: text/html; charset=utf-8
vary: Accept-Encoding
Set-Cookie: T=Ti176942911693100174848747173927528628887308012811447837291709705572; Max-Age=31536000; Domain=flipkart.com; Path=/; Expires=Tue, 26 Jan 2027 12:05:16 GMT; Secure; SameSite=None
Set-Cookie: SN=2.VIB7860695F4D349A3ABE1D107F59D8026.SI97148A5A931D4E21BDC9E9081E09ECC.VSD7F6DFCC59A8440EA4A5D16D422A91E2.1769429116; Max-Age=31536000; Domain=flipkart.com; Path=/; Expires=Tue, 26 Jan 2027 12:05:16 GMT; HttpOnly
Set-Cookie: at=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImQ2Yjk5NDViLWZmYTEtNGQ5ZC1iZDQyLTfkN2RmZTU4ZGNmYS29.eyJleHaiOjE3NzExNTcxMTysImlhCI6MTc20TQyOTEwNiwiXzIijoia2b6FylwianRpijo1ODU2MTfNmNzt61KfUiwiwzElkIjoivEkxNzY5NDI5MTE20TMxMDAxNzQ4NDg3NDcxNz5Mjc1Mjg2Mjg4ODczMdgMTI4MTE0Ndc4MzcyeTE3MdksMDU1NzIiLCJOSWQiOjltYBpividmhiOjJMTyisInoioiJiWUqILCJtIjp0cnVlLCJnZw4iOjR9.sk2YH3GbQU188mxCEv-Kcw_WMTDbSdiosmtPQ2L_1A; Max-Age=31536000; Domain=flipkart.com; Path=/; Expires=Tue, 26 Jan 2027 12:05:16 GMT; HttpOnly
Set-Cookie: K-ACTION=null; Max-Age=31536000; Domain=flipkart.com; Path=/; Expires=Tue, 26 Jan 2027 12:05:16 GMT; HttpOnly
content-security-policy: default-src 'self' https://*.flipkart.com; script-src 'self' 'unsafe-inline' https://*.flipkart.com; script-src 'self' 'unsafe-eval' https://*.flipkart.com https://js-agent.newrelic.com https://bam.nr-data.net https://dpm.demdex.net https://flipkart.d1.sc.omtrdc.net https://www.youtube.com https://vtimg.com http://dpm.demdex.net https://smartplugin.youbora.com https://a-fds.youbarafds01.com https://www.googletagmanager.com https://maps.googleapis.com blob:'nonce-15319257540783298862'; style-src 'self' 'unsafe-inline' https://*.flipkart.com; img-src 'self' * data: blob; media-src 'self' https://*.flipkart.com data: blob; font-src 'self' https://*.flipkart.com data: blob; frame-src 'self' https://*.flipkart.com http://*.flipkart.com https://www.youtube.com https://cdemux.appspot.com blob: fnatcore:/// https://*.flipkart.com https://*.surepass.io; worker-src 'self' https://*.flipkart.com blob:; connect-src 'self' *; base-uri 'self'
x-request-id: BR-c2f3f892-ac18-478d-a838-446ba2cdcbf9
cache-control: private, no-cache, no-store, must-revalidate, max-age=0
expires: Thu, 01 Jan 1970 00:00:00 GMT
pragma: no-cache
etag: bf5214cbdc1c901256ee5b59f6c8b572
last-modified: Wed, 04 Feb 2026 04:47:53 GMT
accept-ch: Sec-CH-UA,Sec-CH-UA-Arch,Sec-CH-UA-Full-Version,Sec-CH-UA-Full-Version-List,Sec-CH-UA-Model,Sec-CH-UA-Platform,Sec-CH-UA-Platform-Version
accept: */*
```

The terminal prompt shows the user is root. The desktop environment includes a file browser window showing various files and folders, and a taskbar with common application icons.

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

# Data Collection & Technology Stack

## Data Collection Method:

- Passive reconnaissance using WHOIS, DNS queries, OSINT tools, and technology fingerprinting
- (No intrusive scanning performed)

## Information Collected:

- Domain and registrar details
- DNS records and IP addresses
- Public subdomains
- HTTP headers and SSL certificate details

## Technology Stack:

### Layer

Frontend

Backend

Server

CDN

Security

Analytics

### Technology

HTML5, JavaScript

Java-based services

Cloud-based servers

Akamai / Cloud CDN

HTTPS, Security Headers

Google Analytics

**CONFIDENTIAL:** The information in this document belongs to Boston Institute of Analytics LLC. Any unauthorized sharing of this material is prohibited and subject to legal action under breach of IP and confidentiality clauses.

# Impact Analysis

## Positive Impact:

- Helps organizations understand exposure
- Improves security posture
- Enables proactive defense

## Negative Impact:

- Attackers map attack surface
- Information leakage risks
- Targeted attacks become easier

# Recommendations & Mitigation Techniques

## Security Measures:

- Hide server banners
- Implement Web Application Firewall (WAF)
- Disable unnecessary services
- Use DNS security (DNSSEC)
- Regular vulnerability scanning

## Best Practices:

- Monitor reconnaissance attempts
- Rate-limit scanning requests
- Apply least-privilege principle
- Conduct regular penetration testing

# Conclusion

- The project demonstrated the importance of reconnaissance as the first phase of cybersecurity assessment.
- Ethical passive reconnaissance tools were used to gather publicly available information about Flipkart.com.
- The analysis showed that Flipkart exposes minimal technical details, indicating a strong security posture.
- Proper use of security mechanisms such as HTTPS, security headers, and CDN reduces information leakage.
- The project concludes that responsible reconnaissance helps organizations identify exposed information and improve security defenses.

# References

- OWASP Foundation – Web Security Testing Guide (Information Gathering) - <https://owasp.org>
- Nmap Project – Network Discovery and Security Auditing Tool - <https://nmap.org>
- Wappalyzer – Web Technology Detection Tool - <https://www.wappalyzer.com>
- DNSDumpster – DNS Reconnaissance & Research Tool - <https://dnsdumpster.co>
- GeeksforGeeks – Cybersecurity and Reconnaissance Concepts - <https://www.geeksforgeeks.org>
- DomainTools – WHOIS Lookup Service - <https://whois.domaintools.com>
- HackerOne – Ethical Hacking & Bug Bounty Platform - <https://www.hackerone.com>
- Google Developers – Robots.txt Specification - [https://developers.google.com/search/docs/crawling-indexing/robots/robots\\_txt](https://developers.google.com/search/docs/crawling-indexing/robots/robots_txt)
- Flipkart Official Website - <https://www.flipkart.com>