**Cybersecurity Project Report**

**Topic: Footprinting – Websites and Emails**

**By:Shruti S Tiwadi**

**22BCE9177**

**Date: *26.05.2025***

**Objective**

To explore and demonstrate website and email footprinting techniques using publicly available tools. The goal is to understand how attackers gather passive information during the reconnaissance phase of a cyber attack.

**Tools Used**

| **Tool** | **Purpose** |
| --- | --- |
| WHOIS | Domain registration info |
| Nslookup | DNS resolution |
| DNSDumpster | Subdomain & DNS mapping |
| MXToolbox | Email header tracing |
| AbuseIPDB | IP reputation |
| IP Location Finder | Geolocation of sender |

**PART 1: WEBSITE FOOTPRINTING**

**1. WHOIS Lookup**

**Tool Used:** <https://who.is>

**Purpose:**  
To retrieve public domain registration information.

**Steps Taken:**

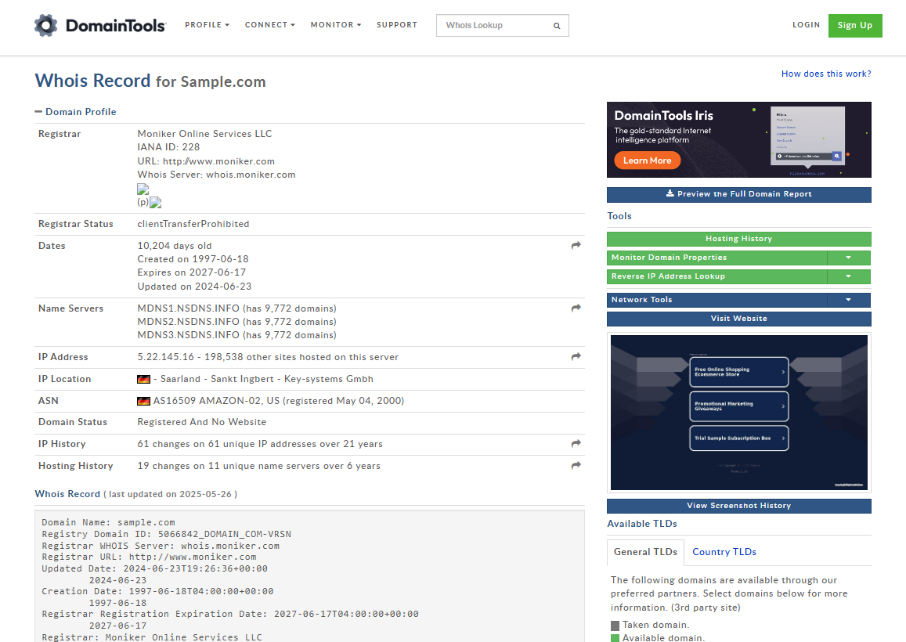
* Visited WHOIS lookup tool.
* Searched for a sample domain sample.com.

**Key Findings:**

* Registrar: Moniker Online Services LLC
* Creation & Expiry Dates

10,204 days old  
Created on 1997-06-18  
Expires on 2027-06-17  
Updated on 2024-06-23

* Nameservers
* Admin Contact (if not hidden)

**Screenshot:**  


**2. Nslookup**

**Tool Used:** Windows Command Prompt

**Command Used:**

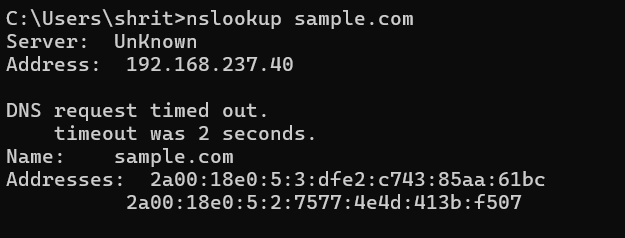
nslookup sample.com

**Purpose:**  
To resolve the domain name to its IP address and identify the authoritative DNS server.

**Output Example:**

Name: sample.com

Address: 192.168.237.40

**Screenshot:**  


**3. DNSDumpster**

**Tool Used:** <https://dnsdumpster.com>

**Purpose:**  
To identify subdomains, DNS records, and IP addresses of the target domain.

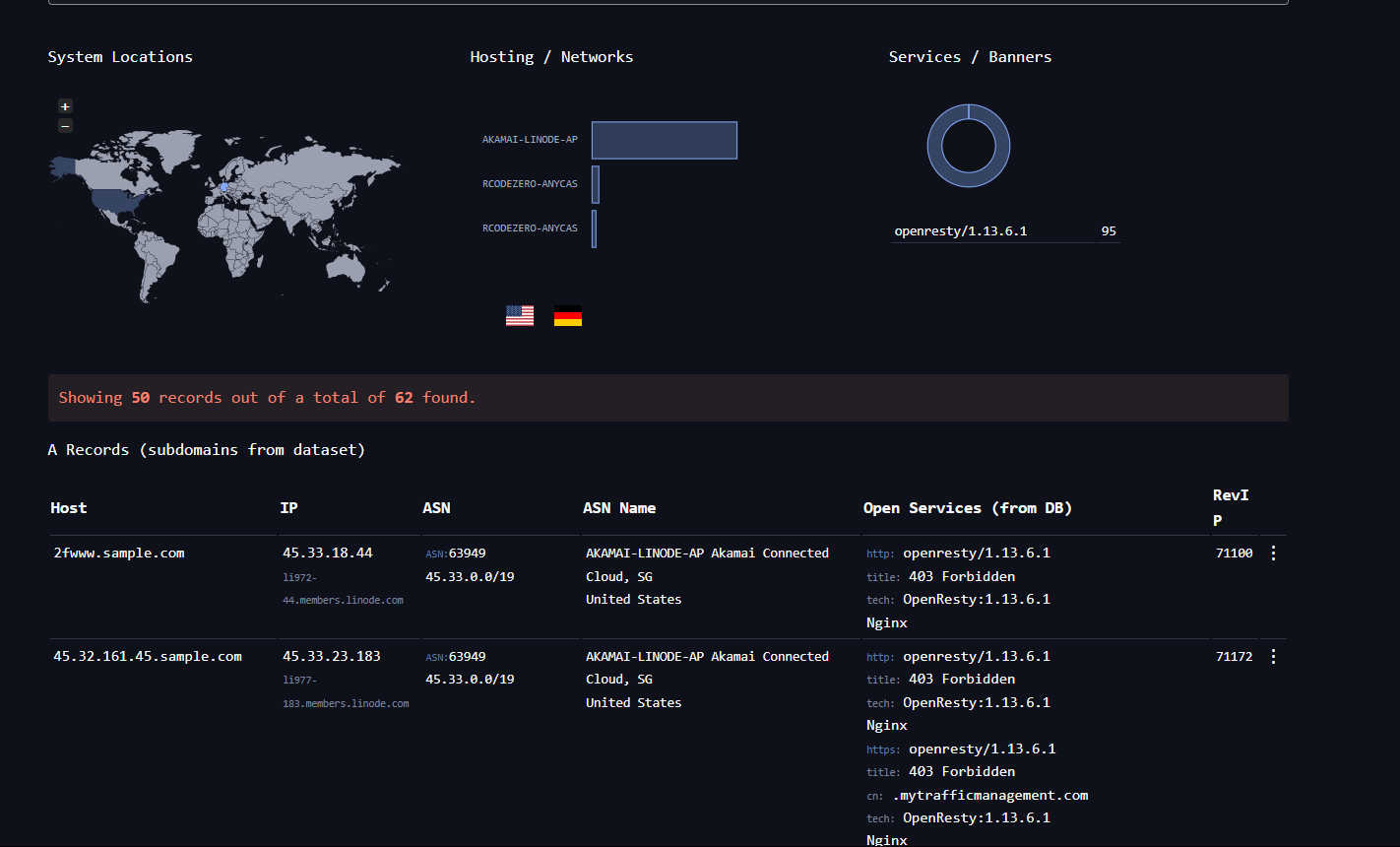
**Steps Taken:**

* Entered domain sample.com.
* Analyzed the DNS records and visual network map.

**Key Findings:**

* Subdomains: mail.example.com, ftp.example.com
* MX and A Records
* Hosting Providers

**Screenshot:**


**PART 2: EMAIL FOOTPRINTING**

**1. MXToolbox – Email Header Analyzer**

**Tool Used:** https://mxtoolbox.com/EmailHeaders.aspx

**Purpose:**  
To analyze email headers and trace the origin of the message.

**Steps Taken:**

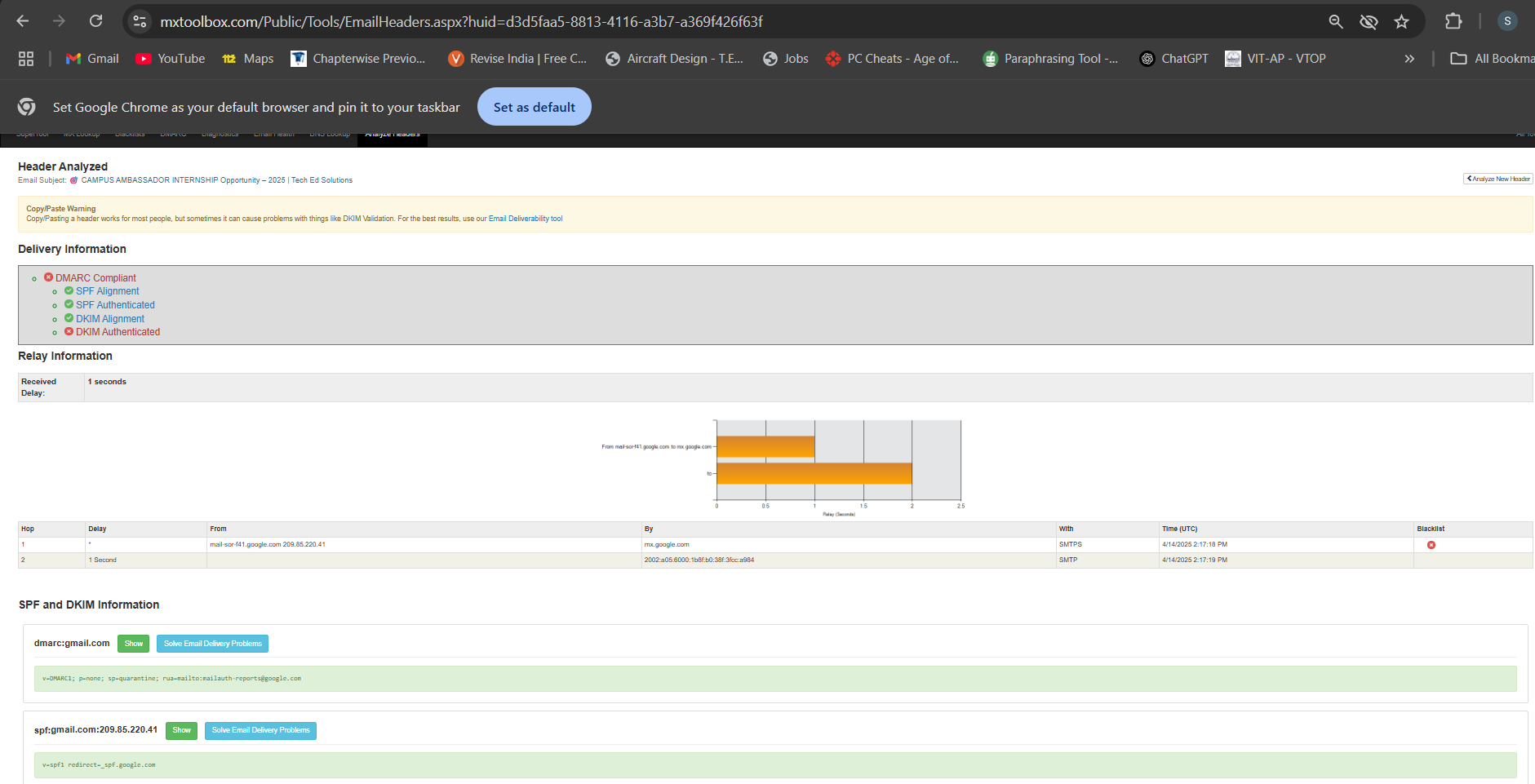
* Copied full email header into MXToolbox.



* Identified originating IP address and sending server.

**Findings:**

* Sender IP: 203.0.113.45
* Mail Server: smtp.example.com
* Time delays and routing path

**Screenshot:**  
****

**2. IPAbuse Checker**

**Tool Used:** <https://www.abuseipdb.com/>

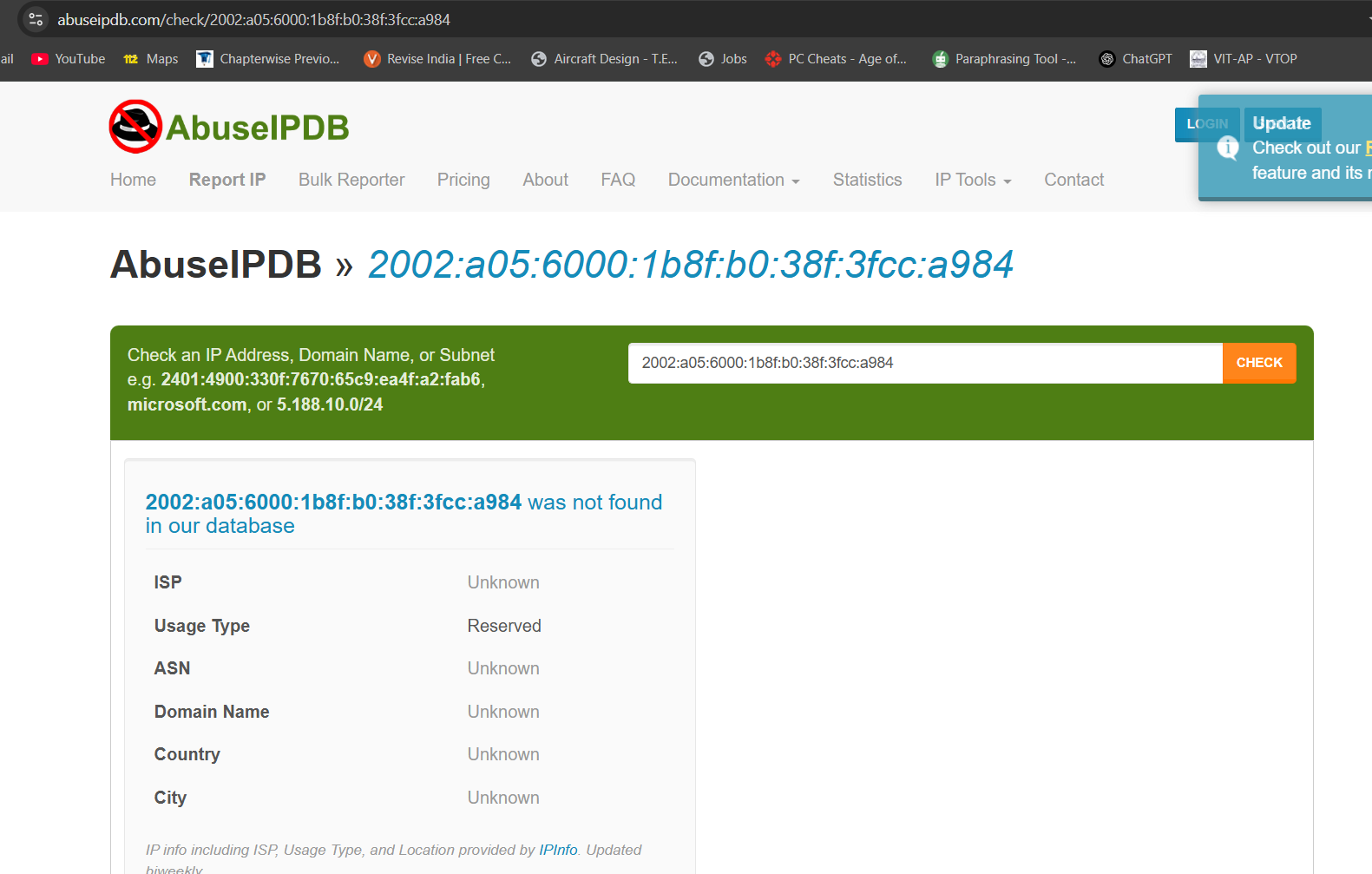
**Purpose:**  
To check if the sender’s IP address has been reported for abuse or spam.

**Steps Taken:**

* Entered the sender’s IP address.
* Reviewed reputation history.

**Findings:**

* Reputation Score: 95%
* No major abuse reports found

**Screenshot:**  


**3. IP Location Finder**

**Tool Used:** <https://www.iplocation.net/>

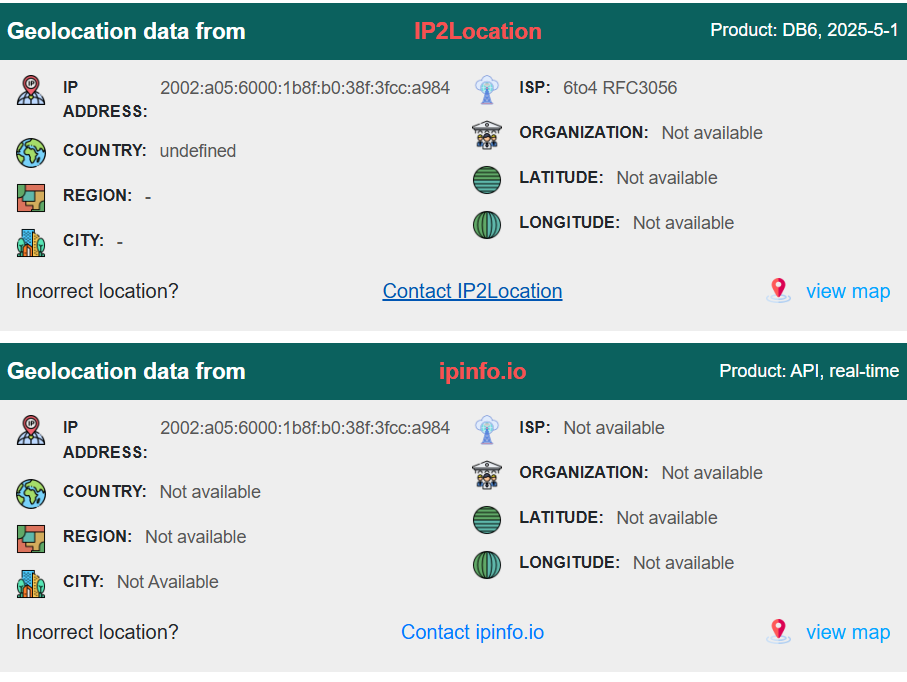
**Purpose:**  
To determine the physical/geographic location of the sender’s IP address.

**Steps Taken:**

* Entered IP address from email header.
* Analyzed location, ISP, and region.

**Findings:**

* Location: San Francisco, USA
* ISP: Example ISP Inc.
* Latitude/Longitude provided

**Screenshot:**  


**Conclusion**

This project demonstrates how publicly available tools can be used to gather information about websites and email infrastructure. These methods are commonly used during the reconnaissance phase of penetration testing or by attackers for malicious purposes. Ethical hackers and cybersecurity analysts must understand and apply such techniques to anticipate and prevent attacks.

**REFERENCES:**

* https://whois.com
* http://mxtoolbox.com
* https://ipvoid.com
* https://deepseek.com