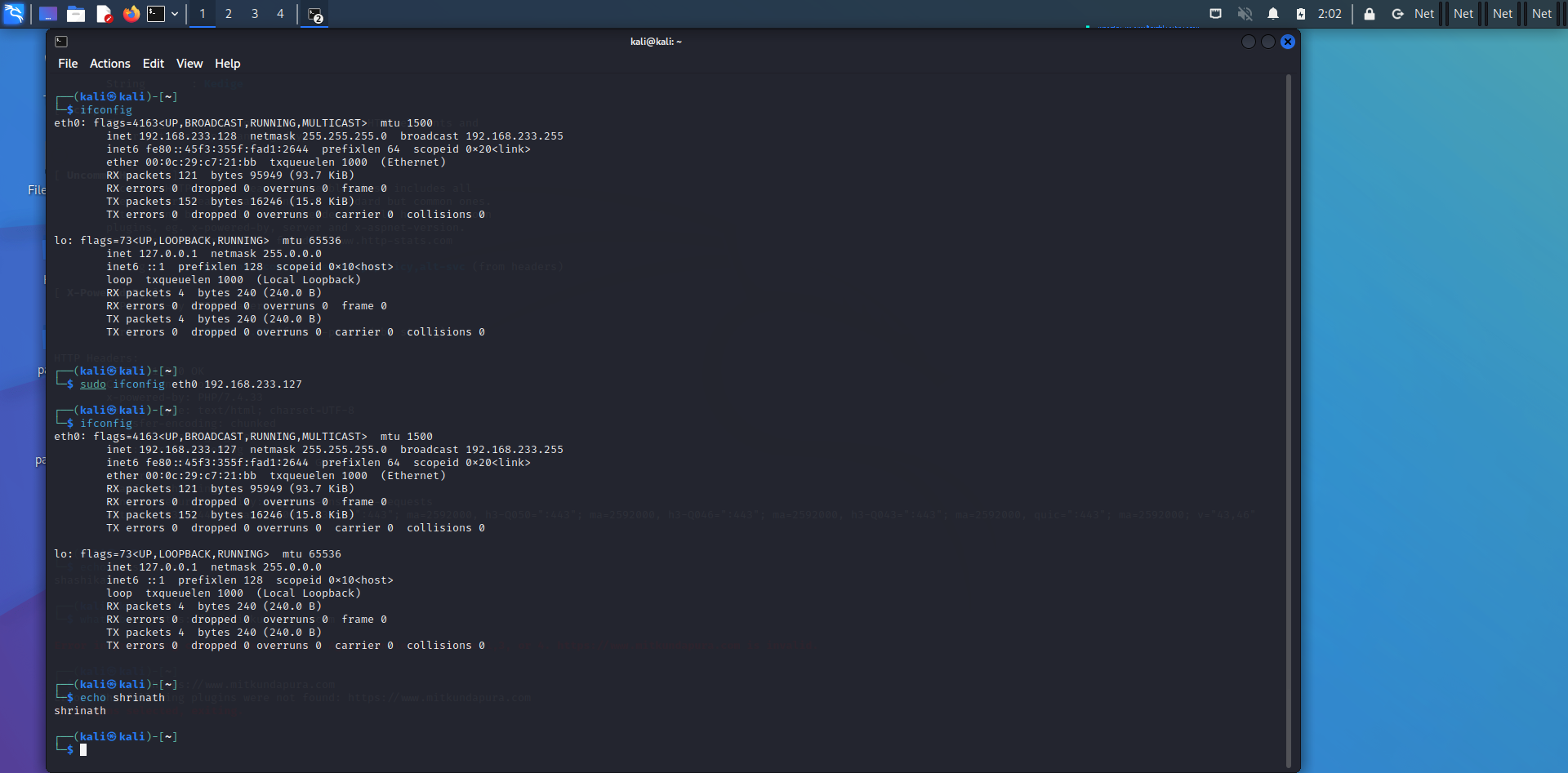
**NAME: SHRINATH**

**DATE:02/03/2023**

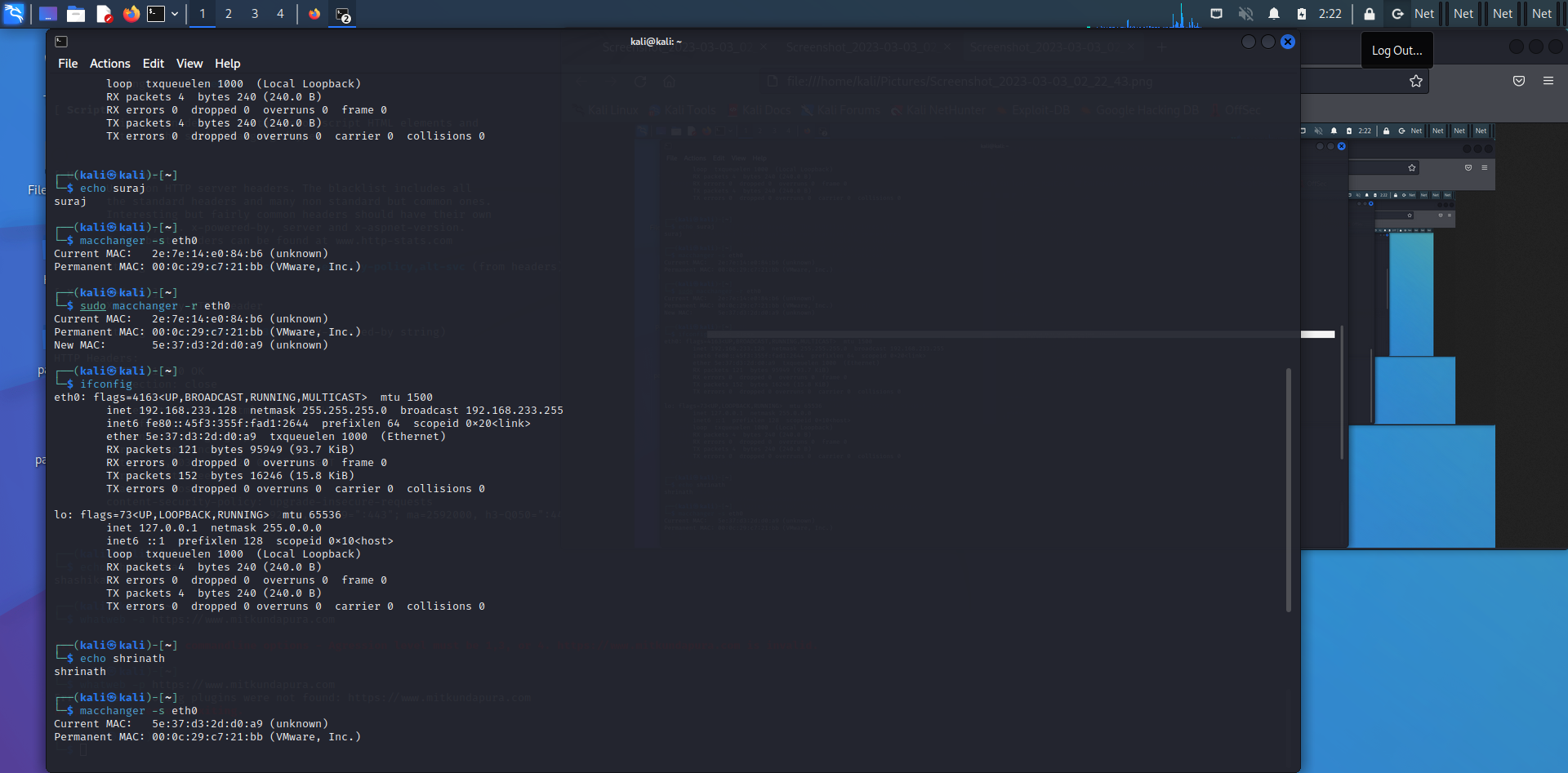
**1)perform ip address spoofing:**

IP address spoofing is a technique used by attackers to manipulate the source address of a network packet to conceal their identity or impersonate another system.



**2) Perform mac address spoofing:**

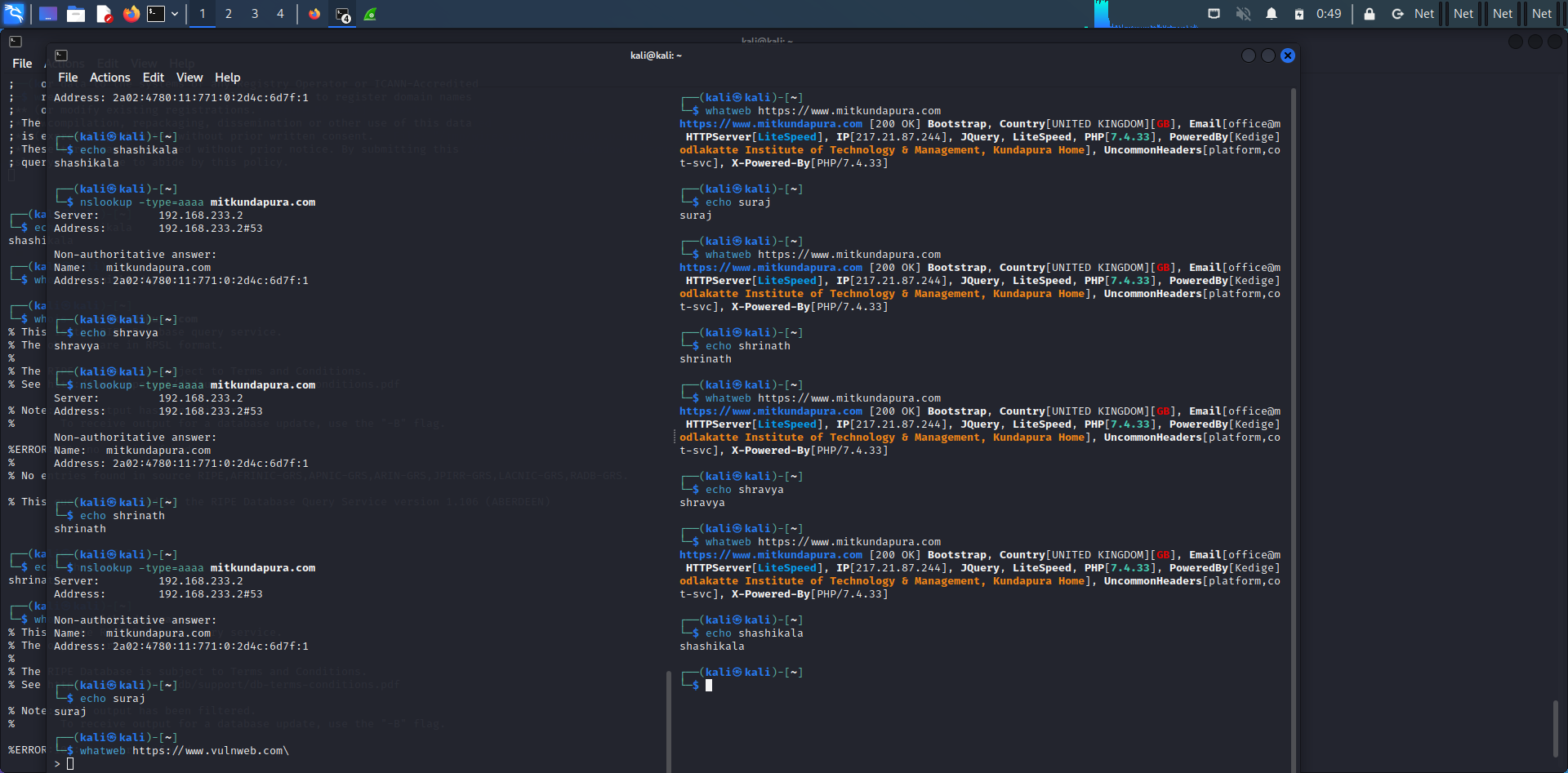
MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address that is hard-coded on a network interface controller (NIC) cannot be changed. However, many drivers allow the MAC address to be changed.



**3) Any 5 whatweb commands:**

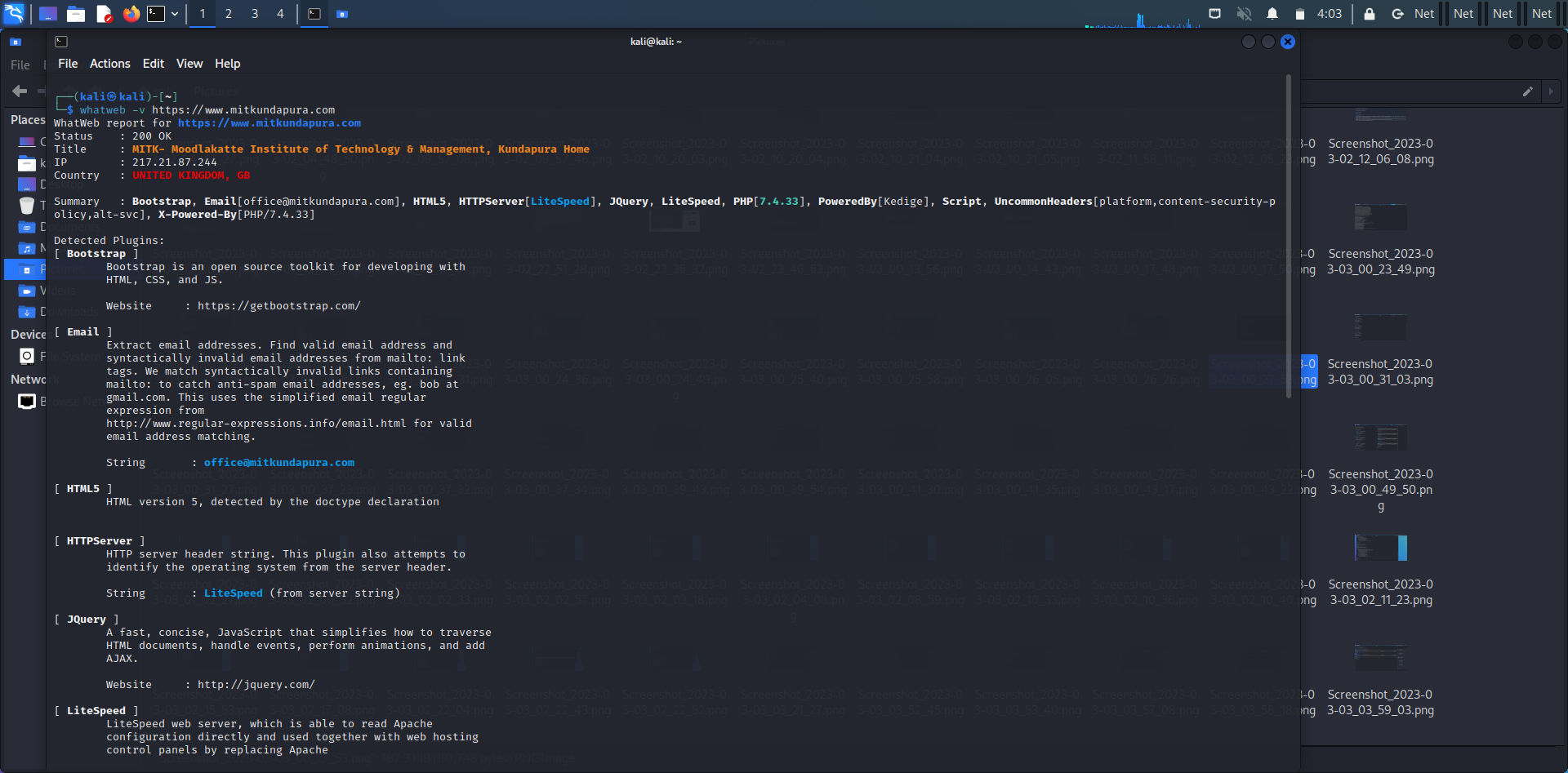
Basic scanning: The most basic command to scan a website with WhatWeb is

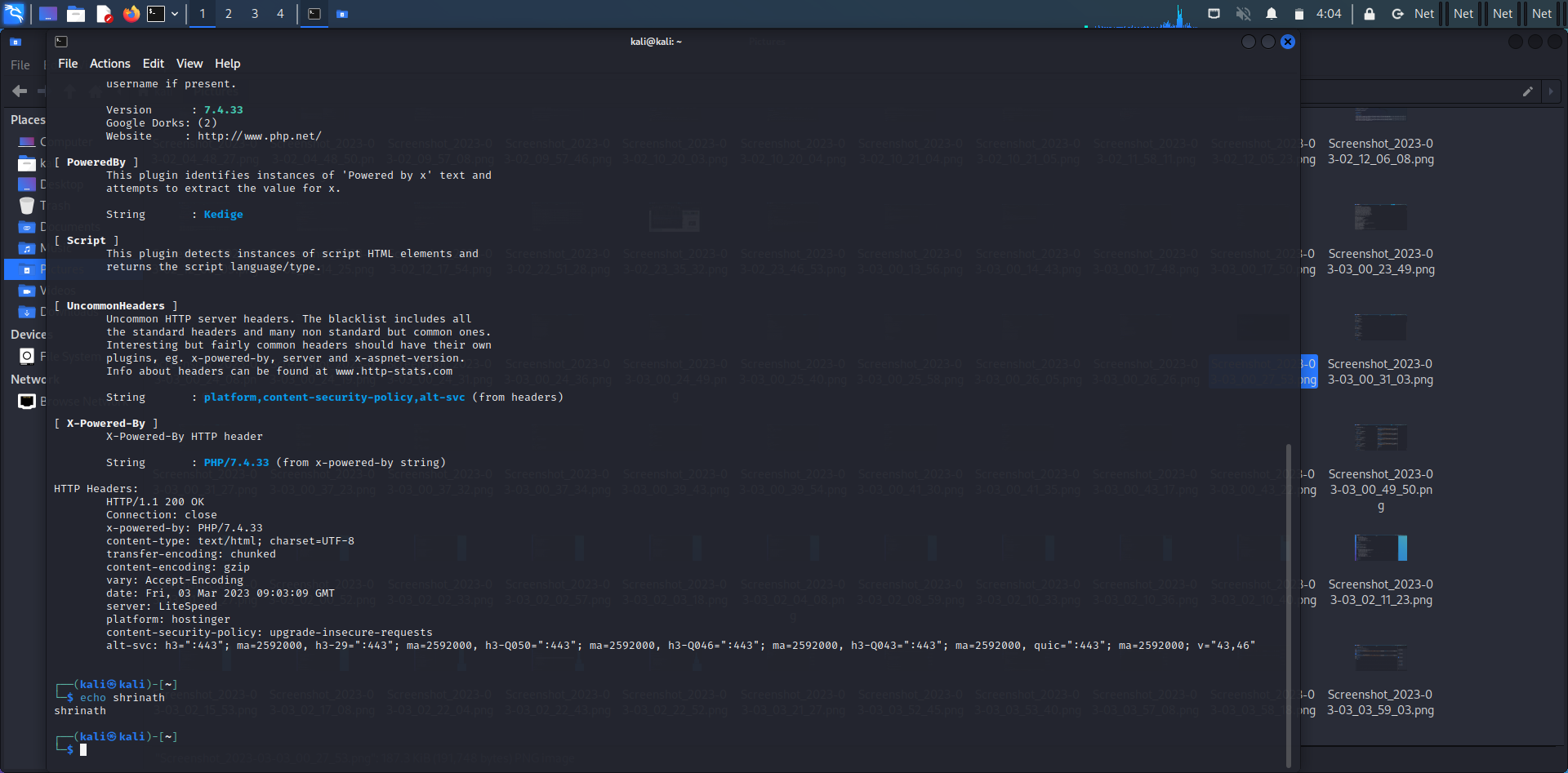
**$ whatweb mitkundapura.com**



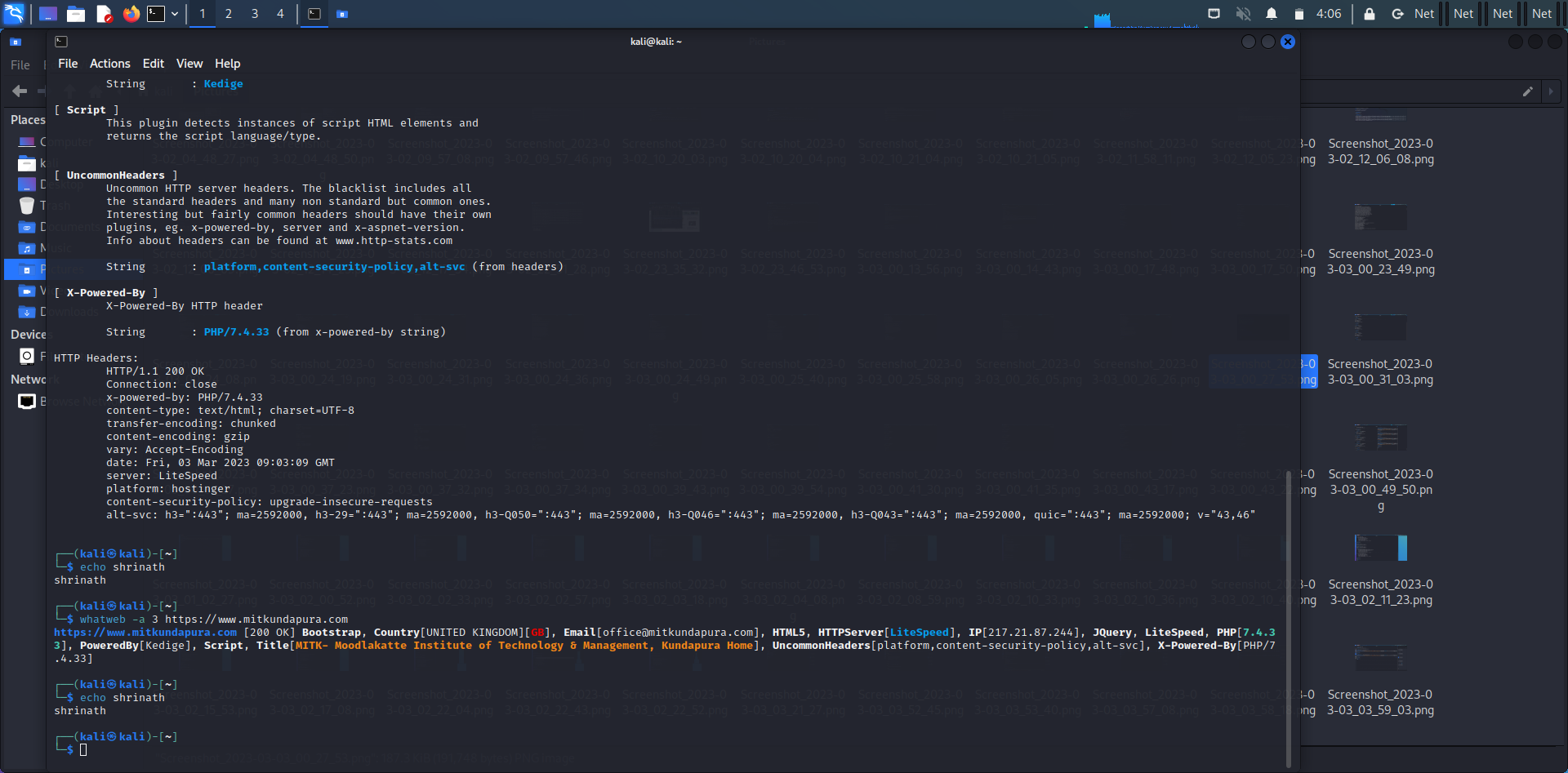
Verbose scanning: If you want more detailed information about the website, you can use the verbose flag (-v):

**$ whatweb -v mitkundapura.com**

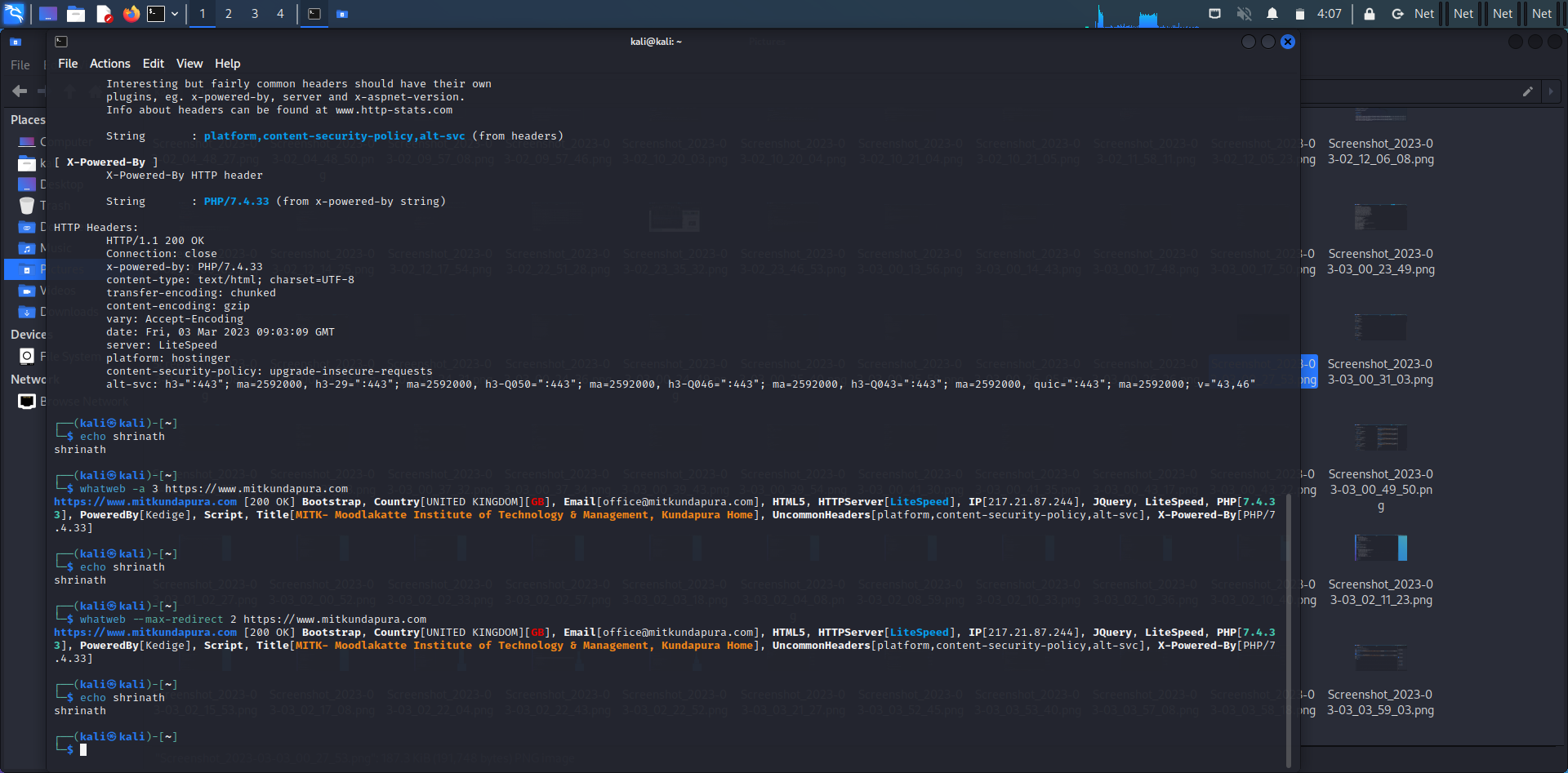




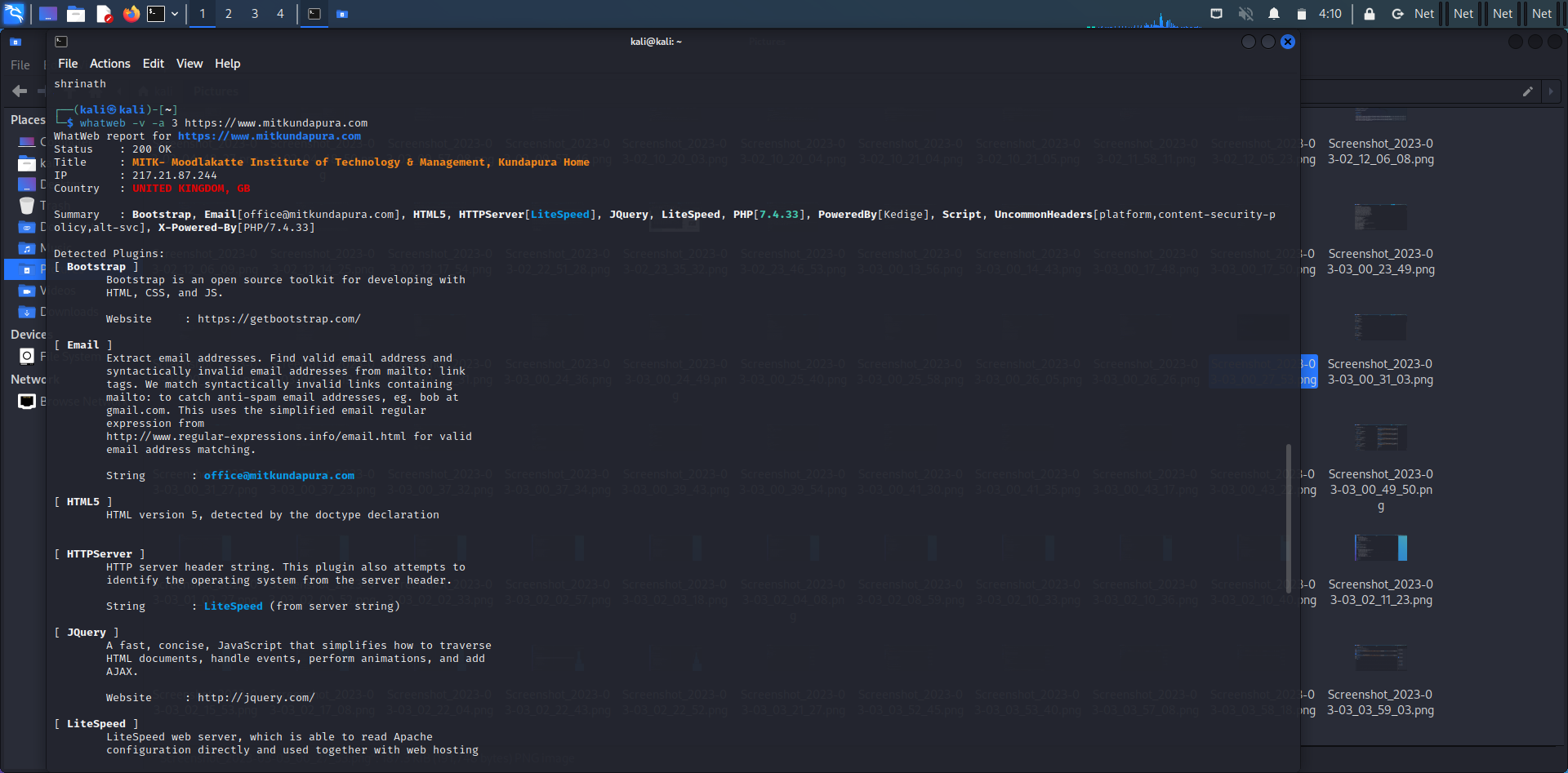
**$whatweb -a 3 https://www.mitkundapura.com**

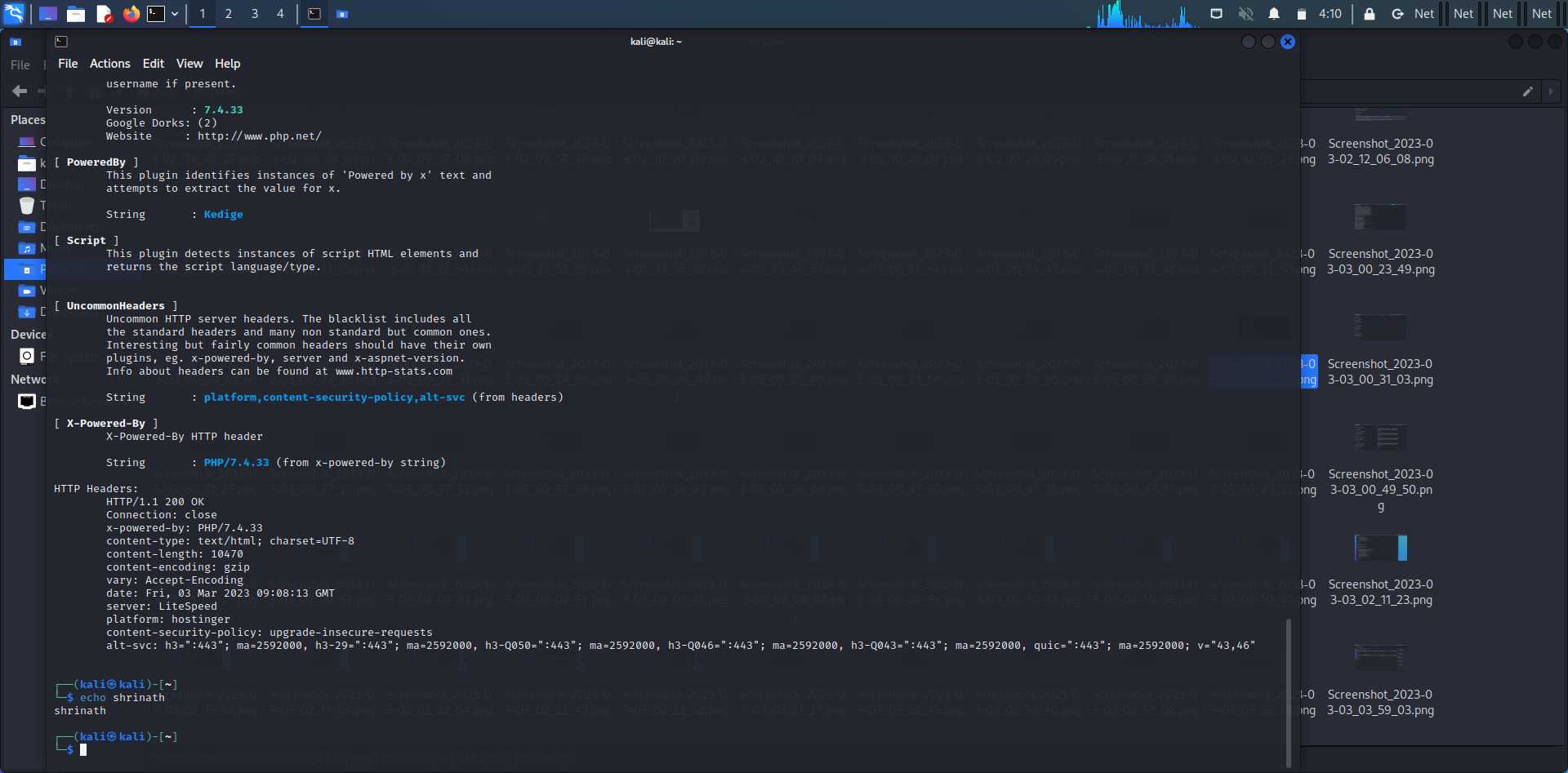


**$whatweb --max-redirect 2 https://www.mitkundapura.com**



**$whatweb -v -a -3 https://www.mitkundapura.com**



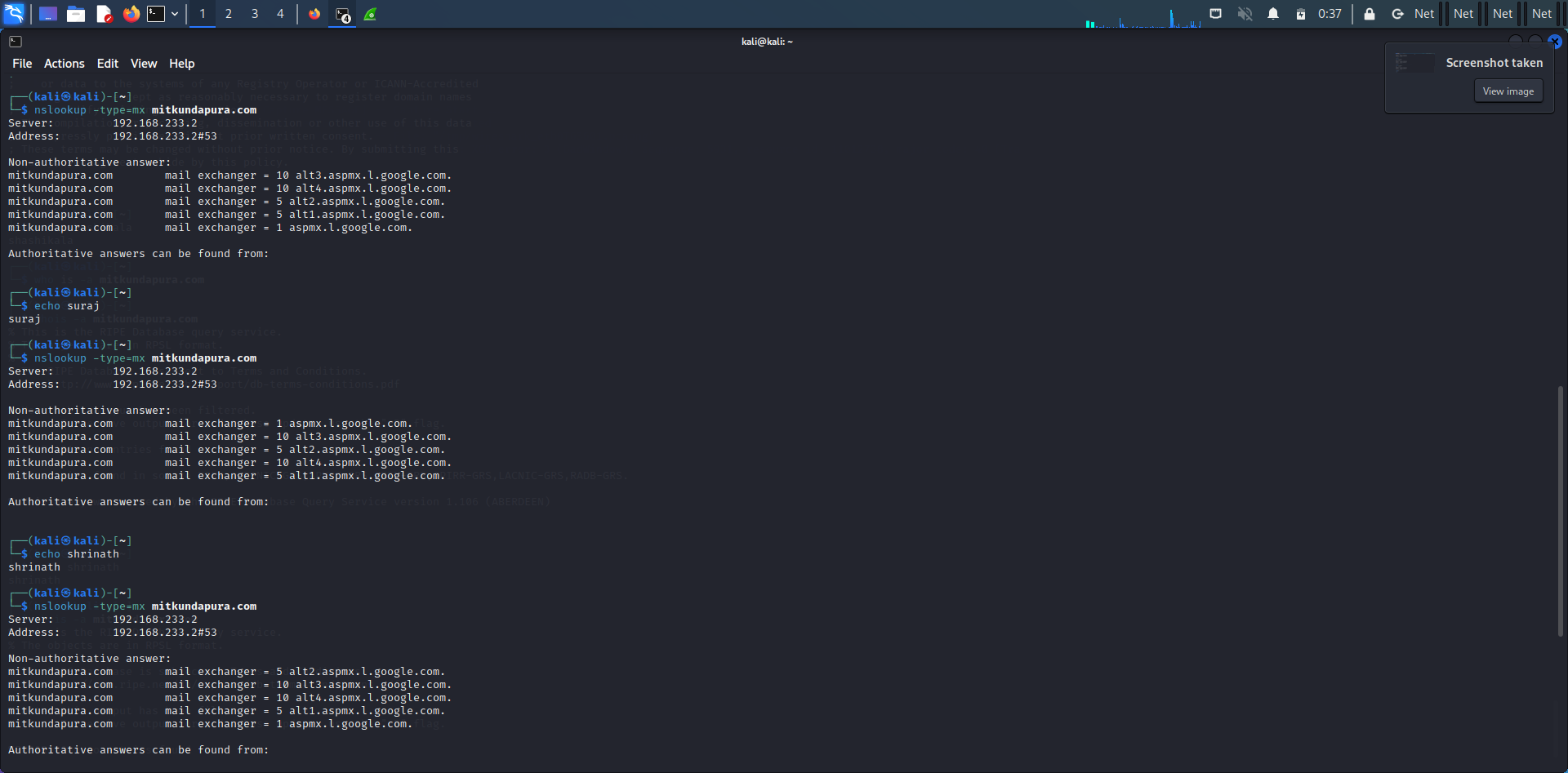


4) **$ nslookup google.com:**



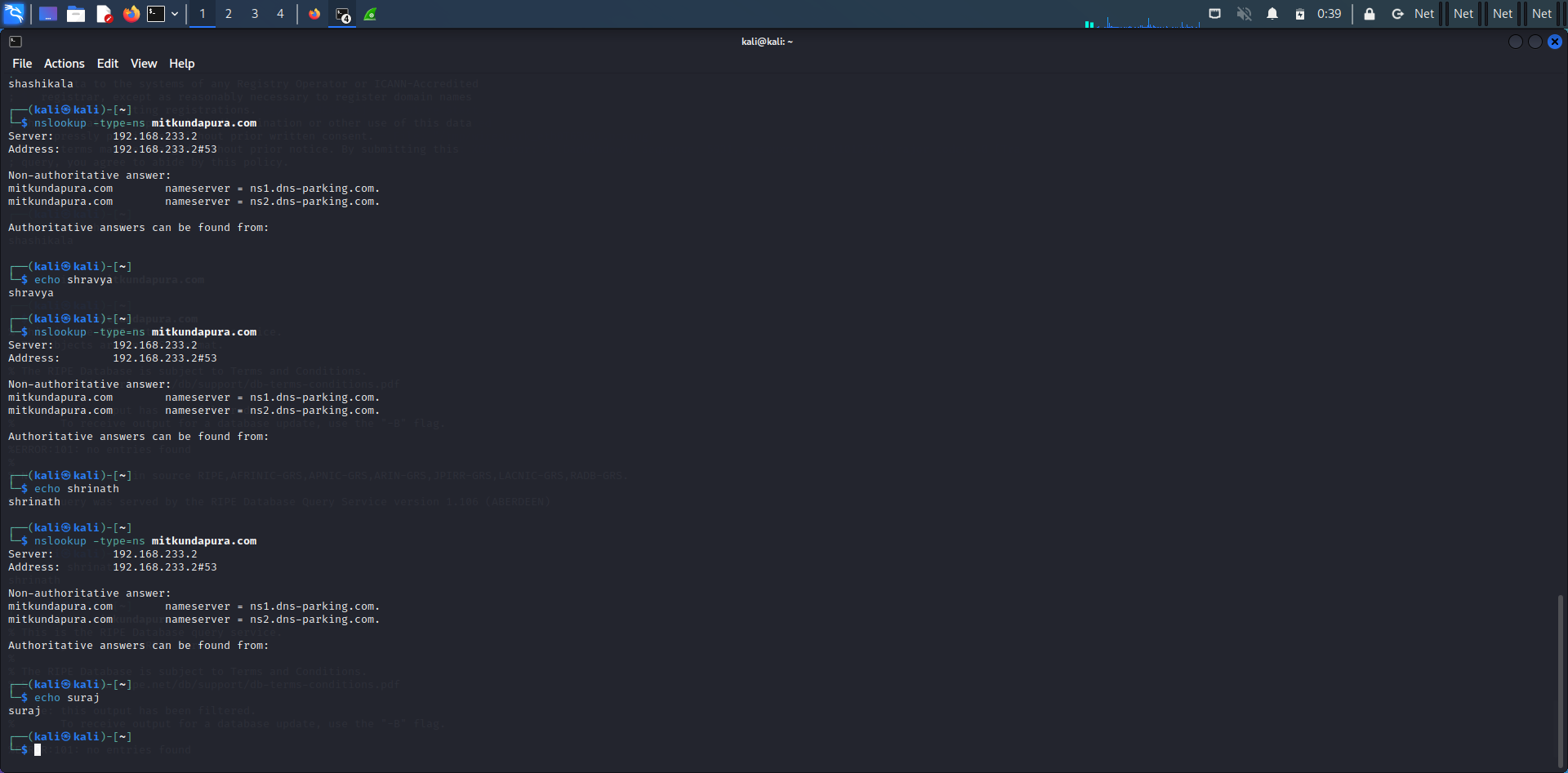
**$ nslookup -type=mx mitkundapura.com**

This command will perform a DNS lookup for the mail exchange (MX) records associated with the domain name “example.com”.



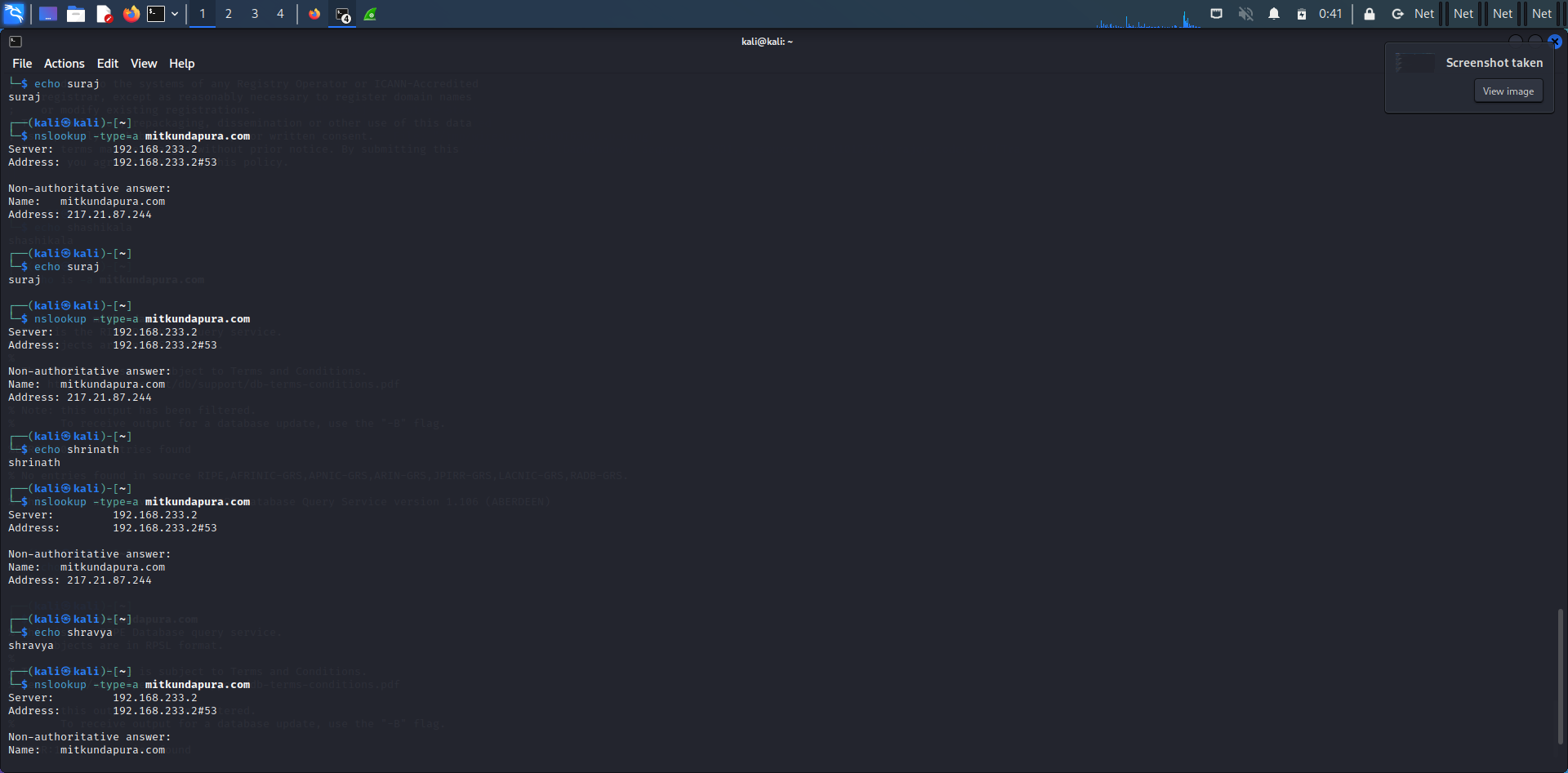
**$ nslookup -type=ns mitkundapura.com**

This command will perform a DNS lookup for the name server (NS) records associated with the domain name “example.com”.

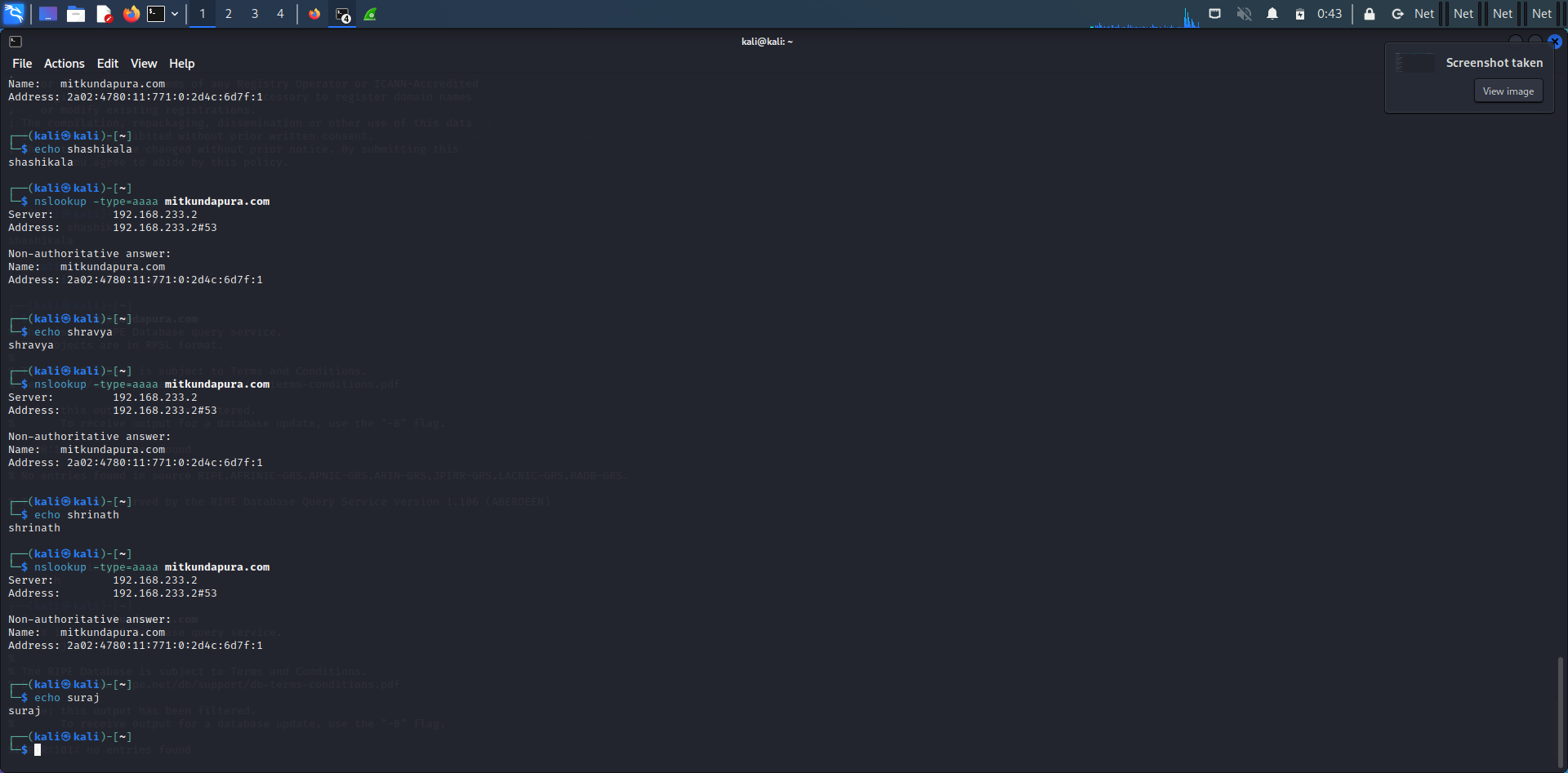


**$ nslookup -type=a mitkundapura.com**

This command will perform a DNS lookup for the IPv4 address associated with the subdomain www.example.com.



**$ nslookup -type=aaaa mitkundapura.com**

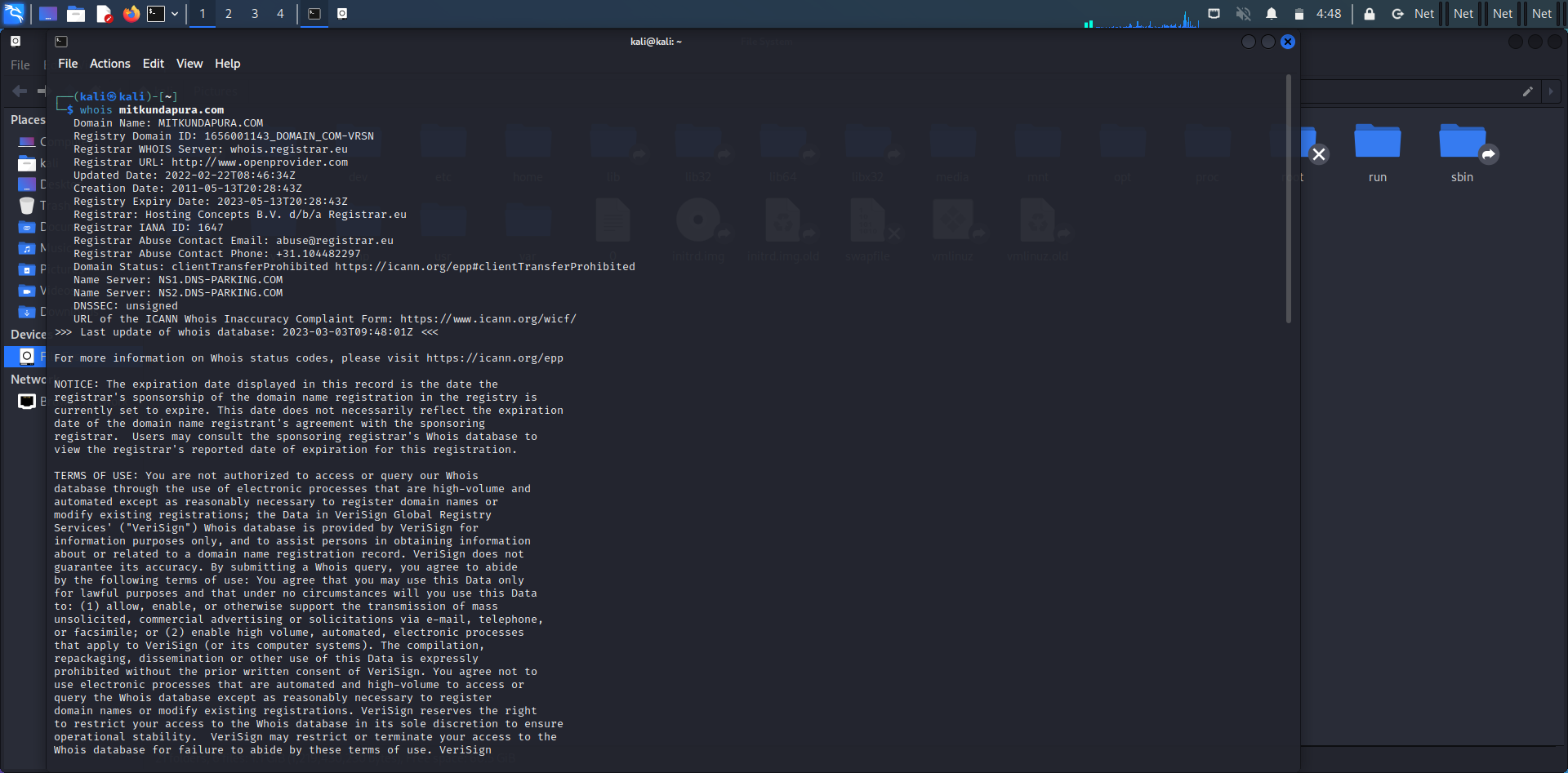


**5) whois command:**

The WHOIS command is a network administration utility used to obtain information about a domain name, IP address or an autonomous system number (ASN) on the Internet. It allows you to look up information about the registered owner of a domain name, including the domain's registrar, date of registration, expiration date, and contact details.

**$ whois mitkundapura.com**

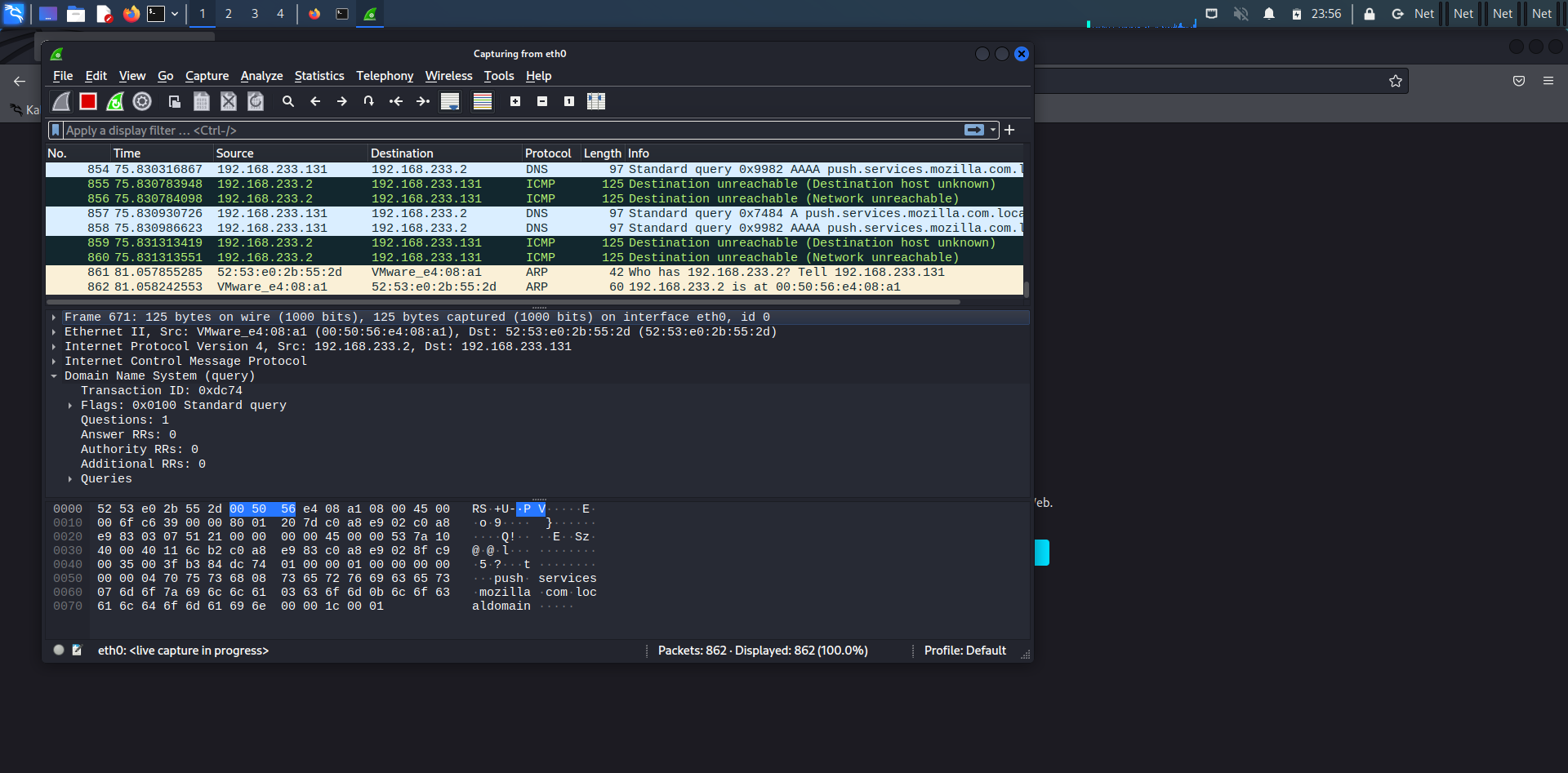
This command will display information about the domain name, such as the name of the registrant, the name servers, and the date of registration





**6) Find data packets using wireshark:**

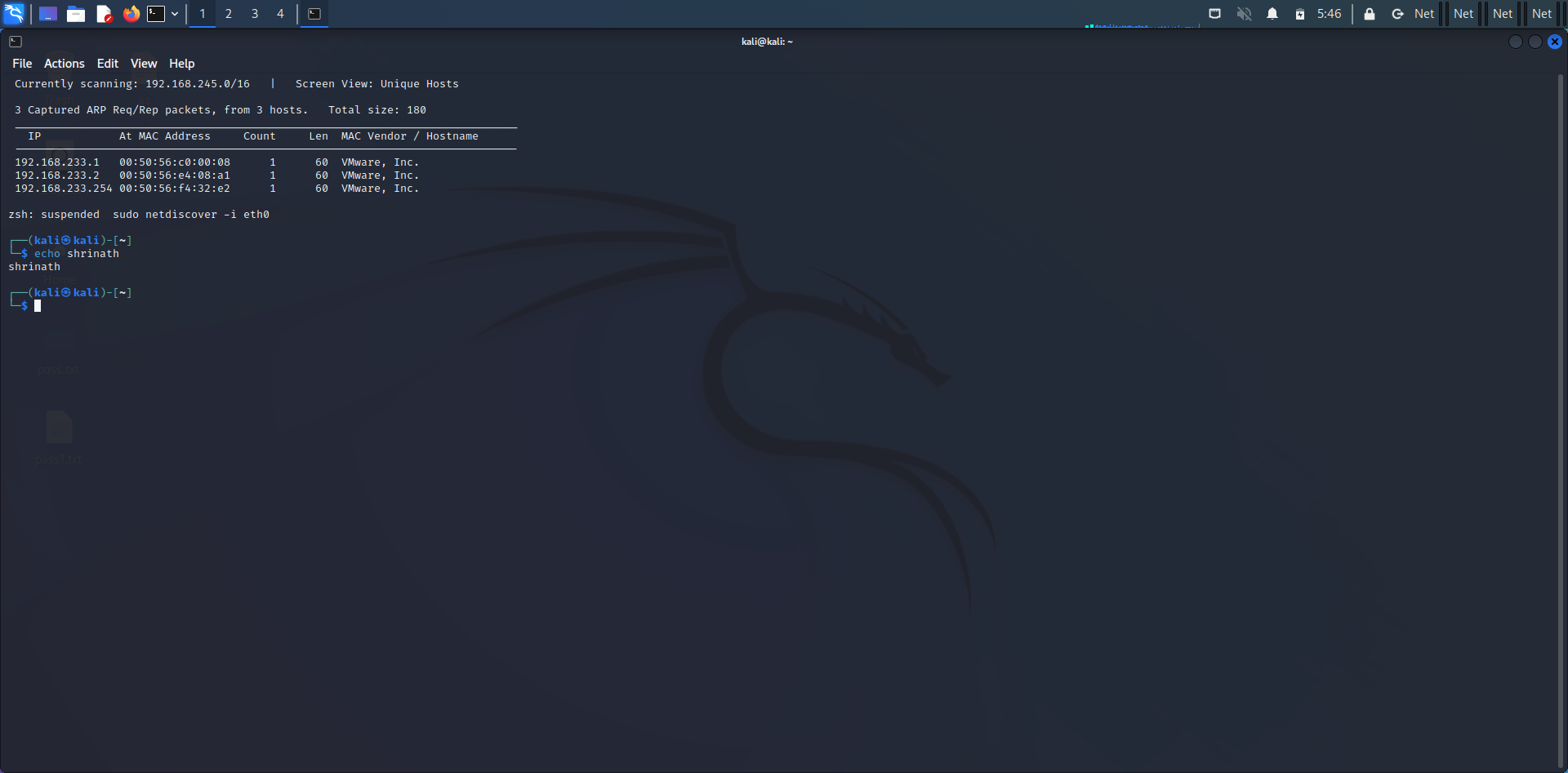
Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network. Wireshark is the most often-used packet sniffer in the world.



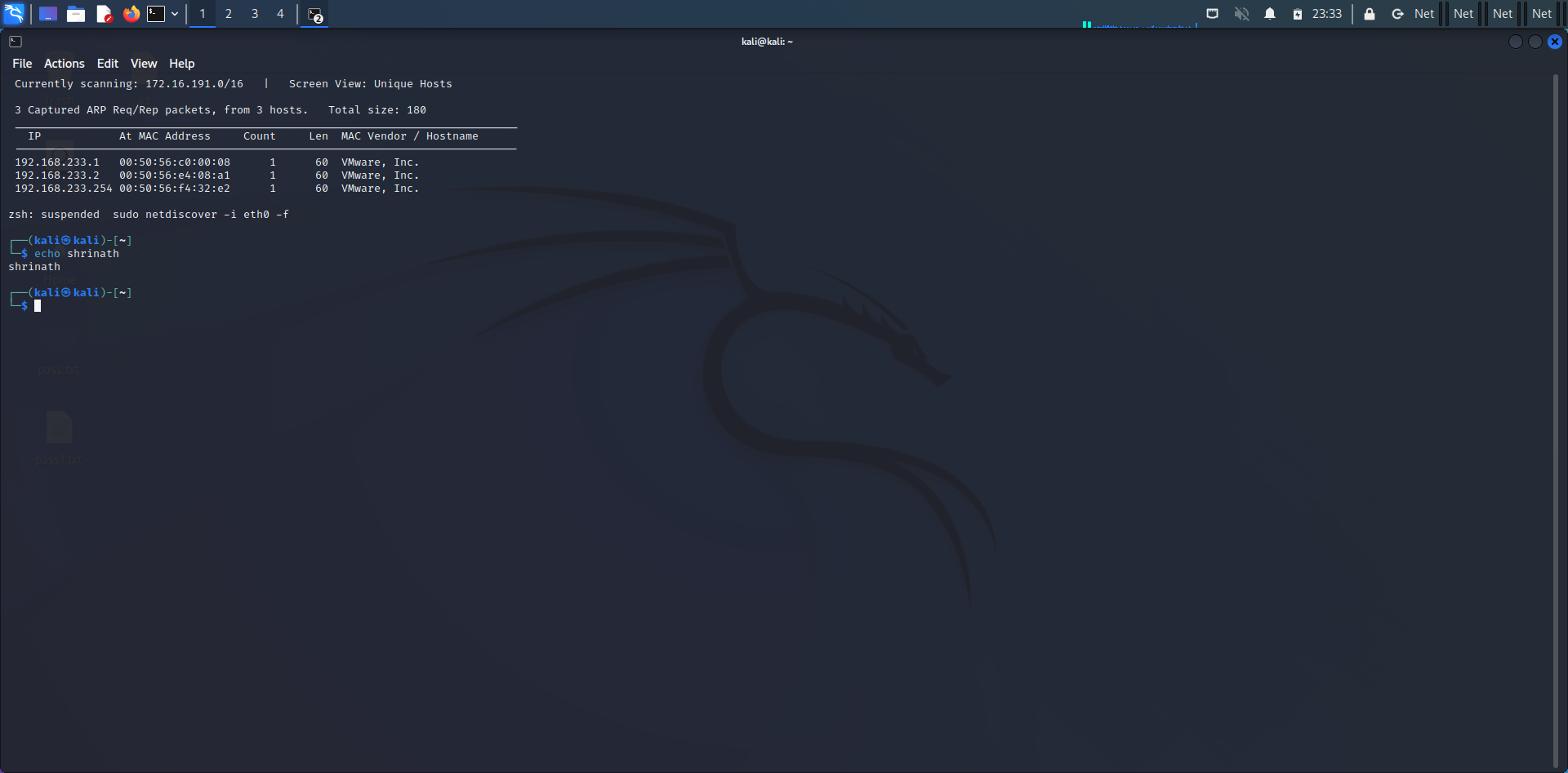
**7) Any 5 netdiscover command:**

Netdiscover is a network scanning tool used for discovering hosts and gathering information about them on a local network. Here are some of the basic commands:

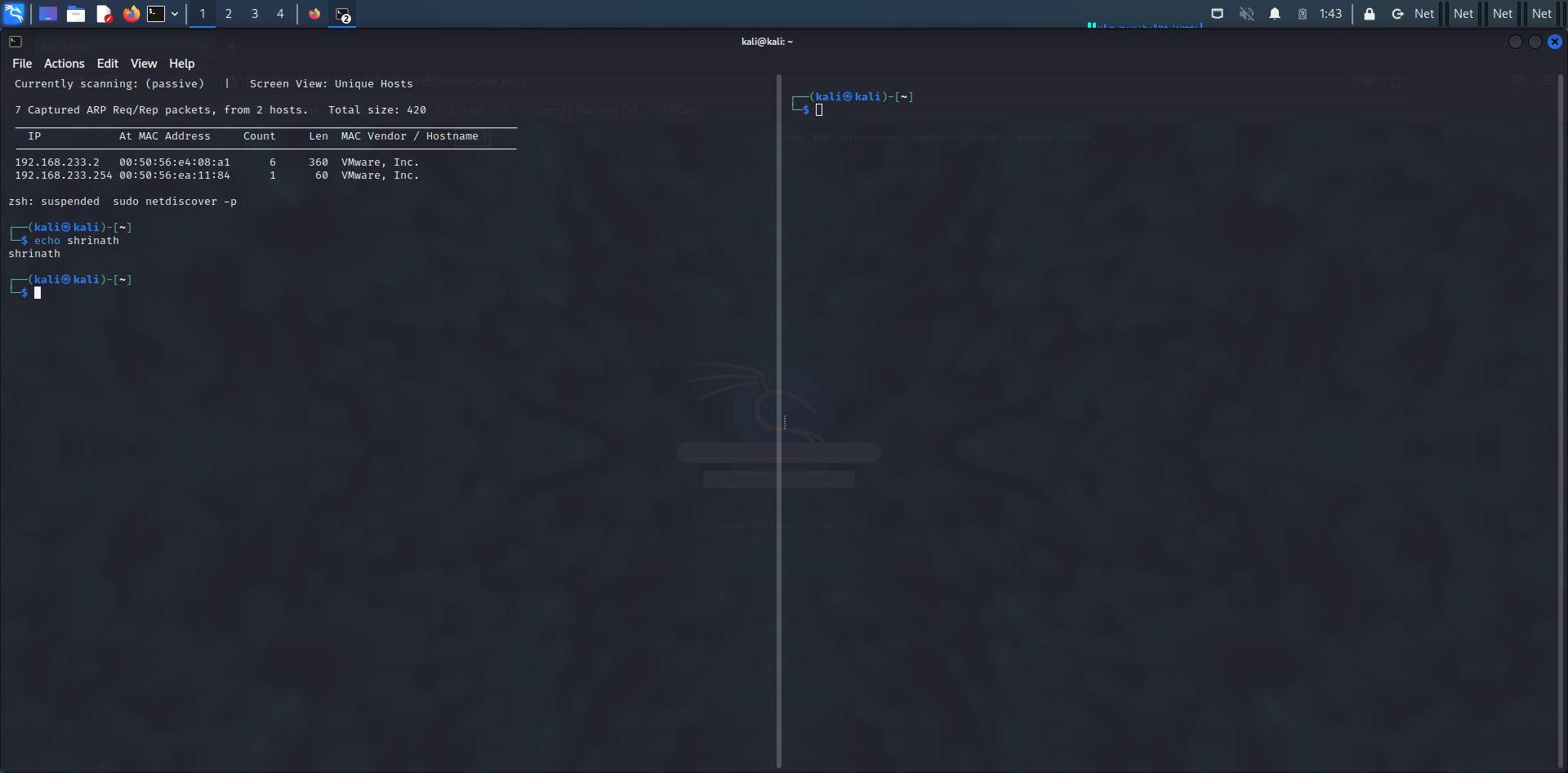
**$ netdiscover -i eth0**



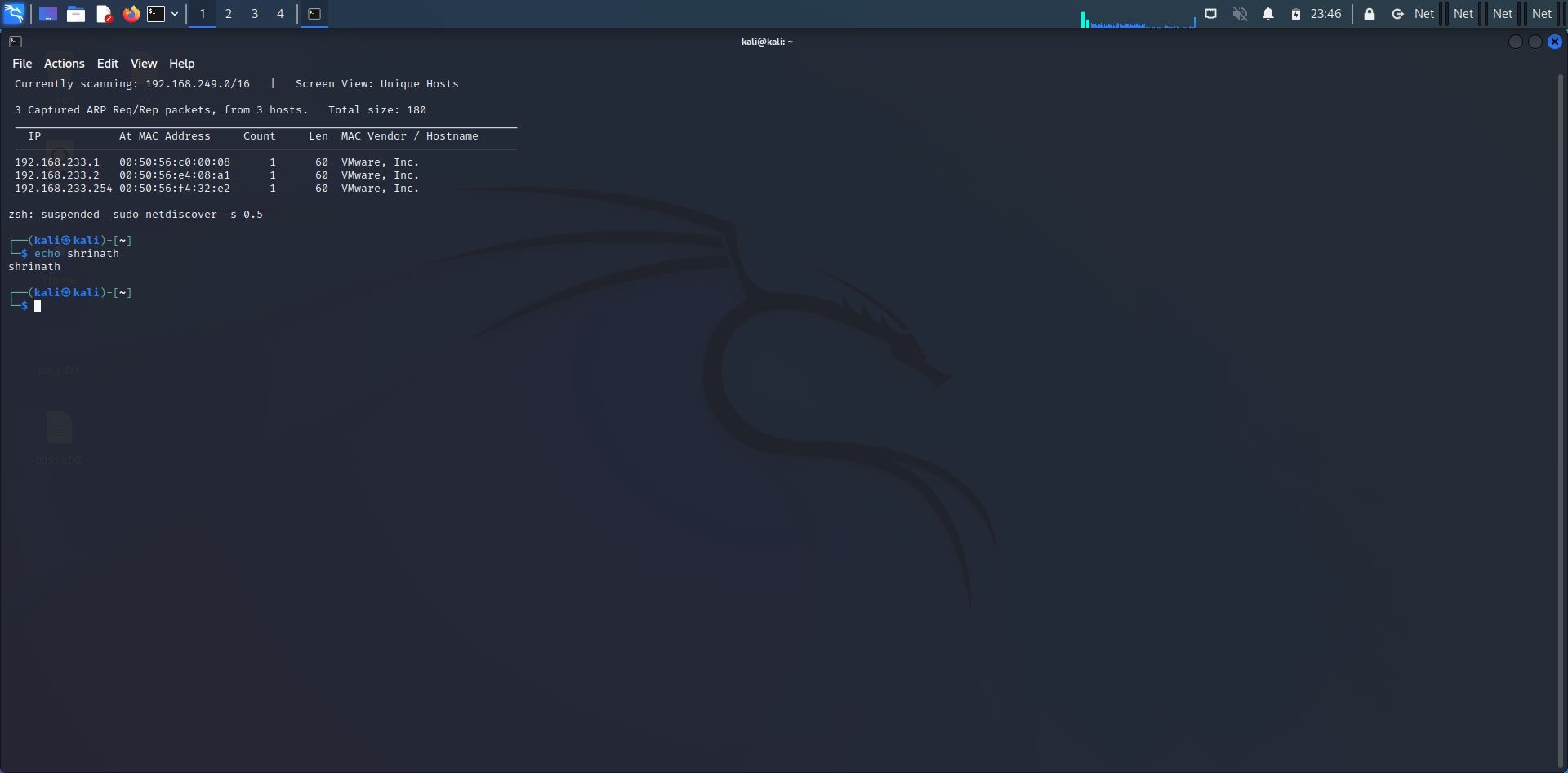
**$ netdiscover -i eth0 -f**



**$ netdiscover -p**

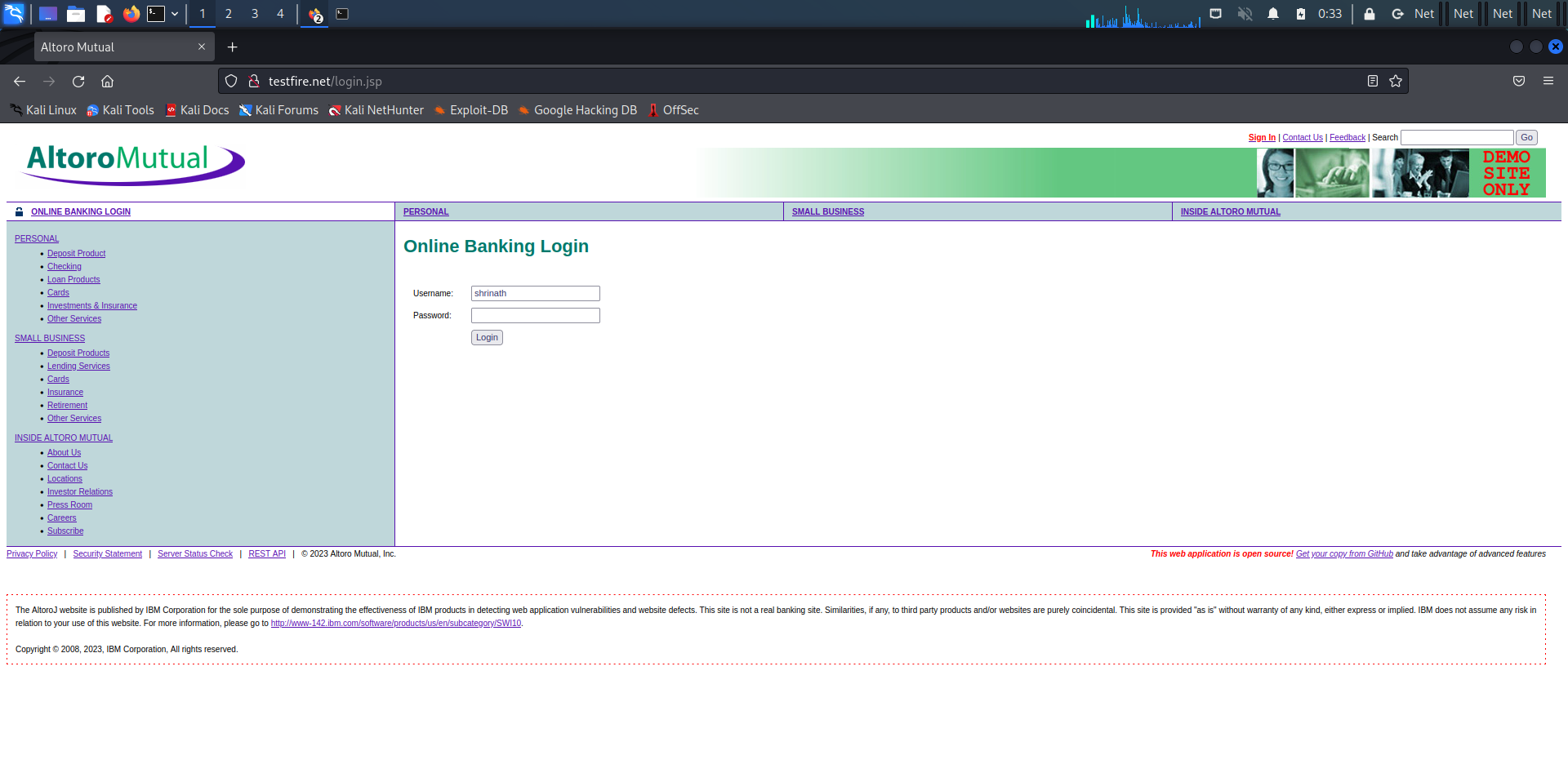


**$ netdiscover –s 0.5**



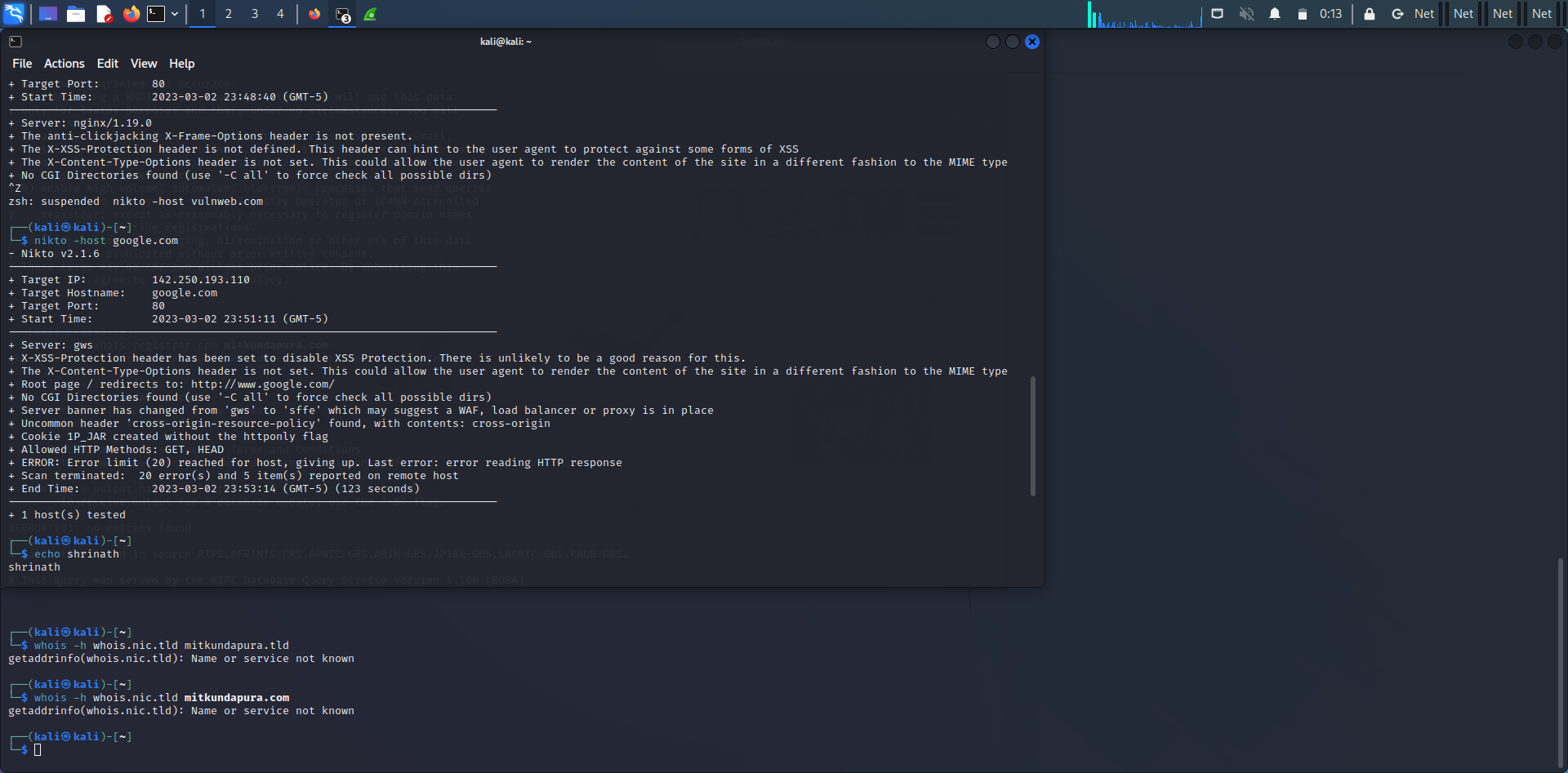
**8) CryptoConfiguration flaw :**

A crypto configuration flaw refers to a security vulnerability that occurs due to improper configuration of cryptographic settings in a system or application. Cryptography is the science of using mathematical algorithms to protect data from unauthorized access or modification, and it is an essential component of modern computer security.



**9) Nikto commands**:

Nikto is a free software command-line vulnerability scanner that scans webservers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received.



**10) Find xml pages in website using dirbuster:**

DirBuster is a multithreaded java application designed to brute force directories and files names on web/application servers. Often is the case now of what looks like a web server in a state of default installation is actually not, and has pages and applications hidden within

