**NAME : SHASHIKALA**

**DATE : 02-03-2023**

**TASK-2**

**1)Perform IP address spoofing:**

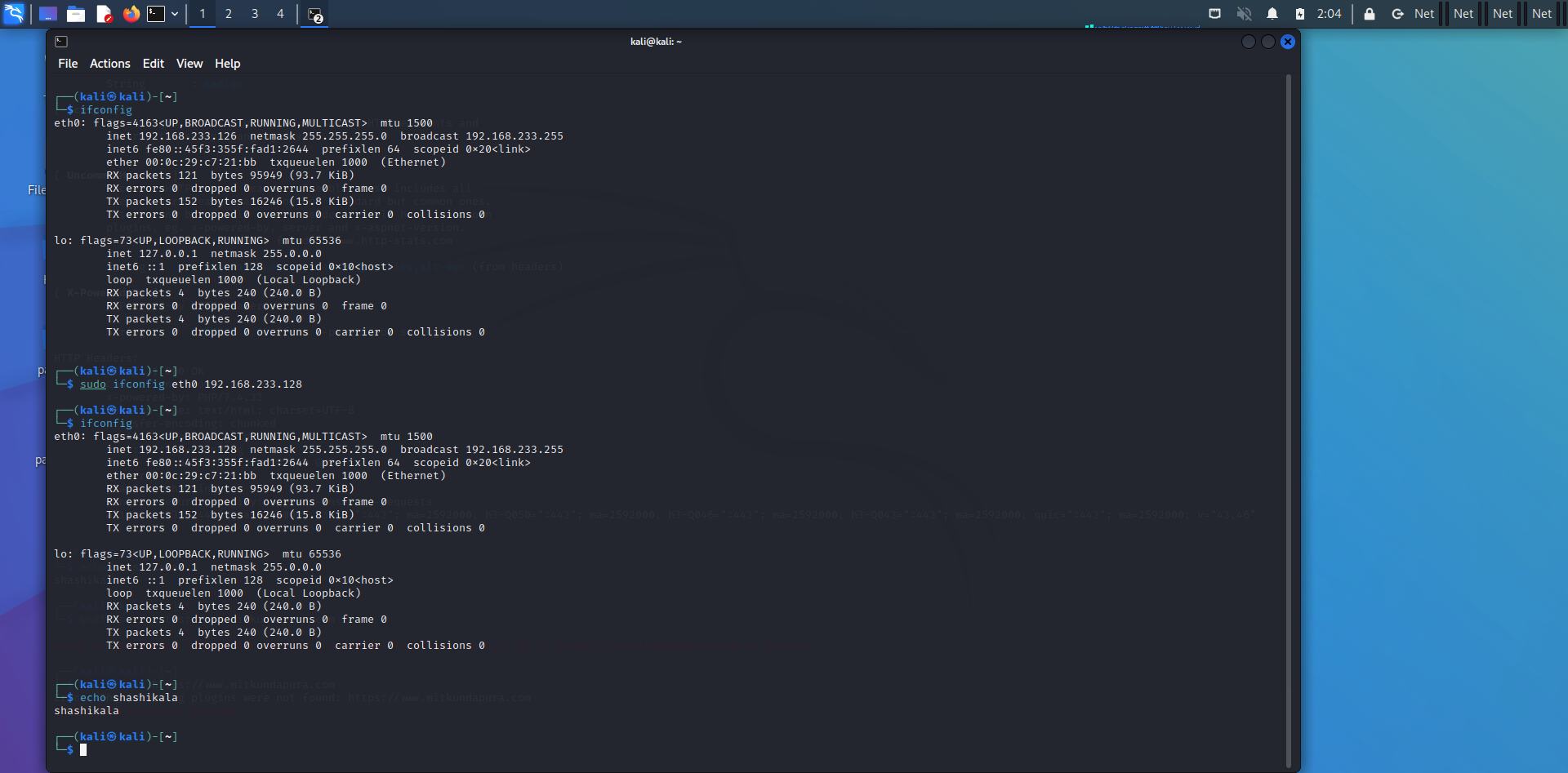
IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a false source IP address, for the purpose of impersonating another computing system.

**Command:**

$ ifconfig

$ sudo ifconfig eth0 192.168.233.126

$ ifconfig



**2)Perform Mac address spoofing:**

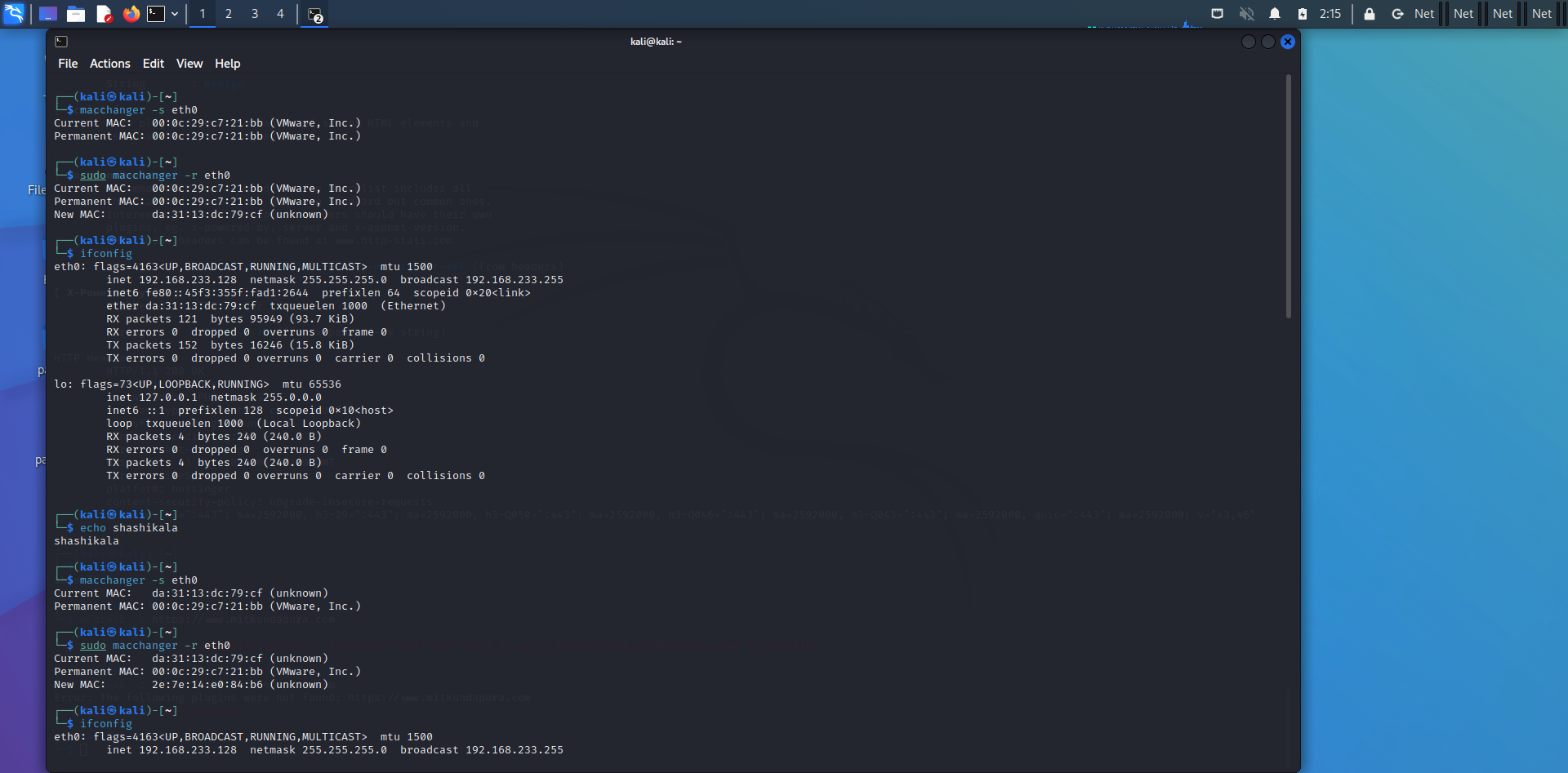
MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address that is hard-coded on a network interface controller (NIC) cannot be changed. However, many drivers allow the MAC address to be changed.

**Command:**

$ macchanger -s eth0

$ sudo macchanger -r eth0

$ ifconfig

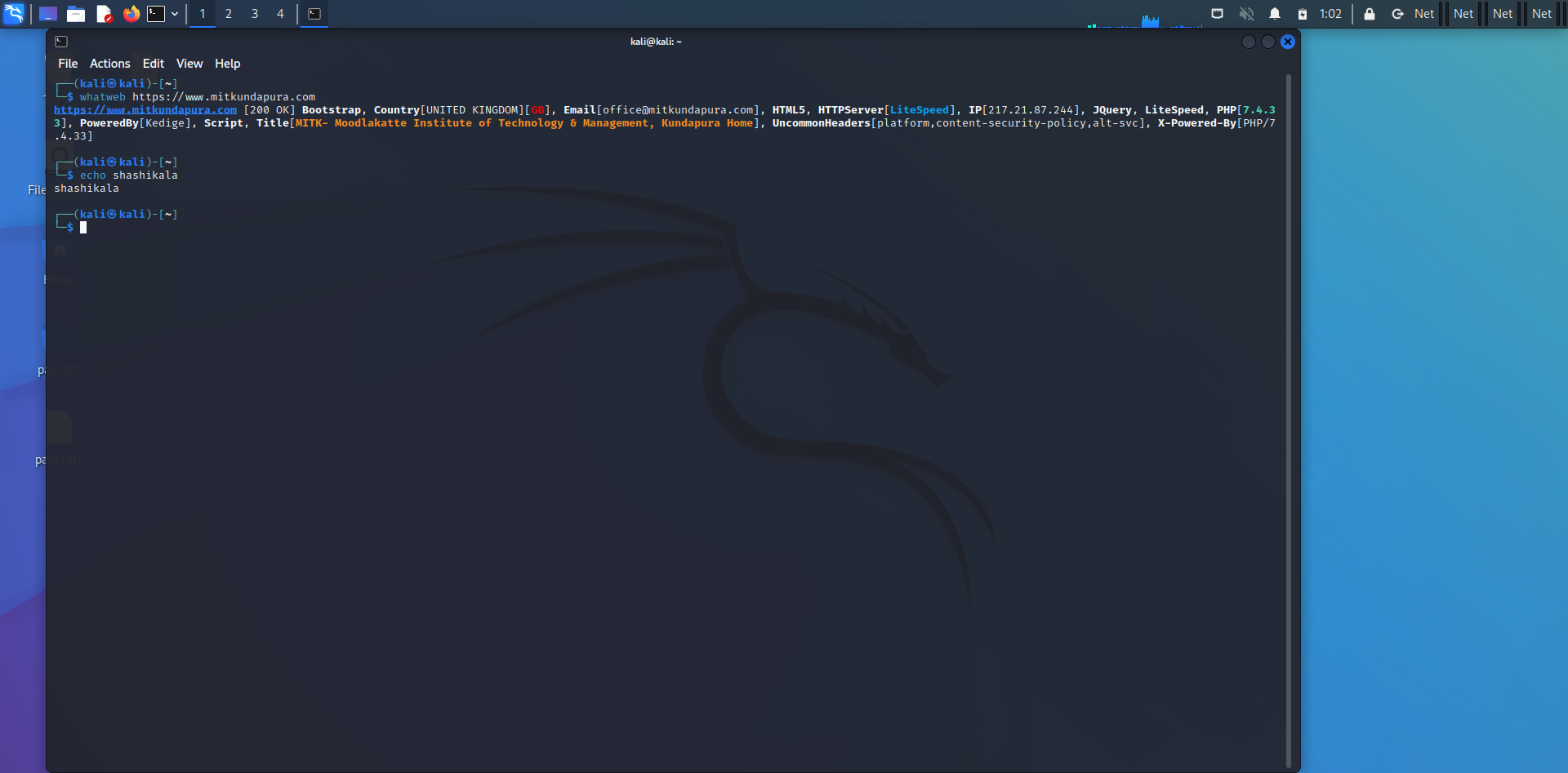


**3)Any 5 Whatweb commands:**

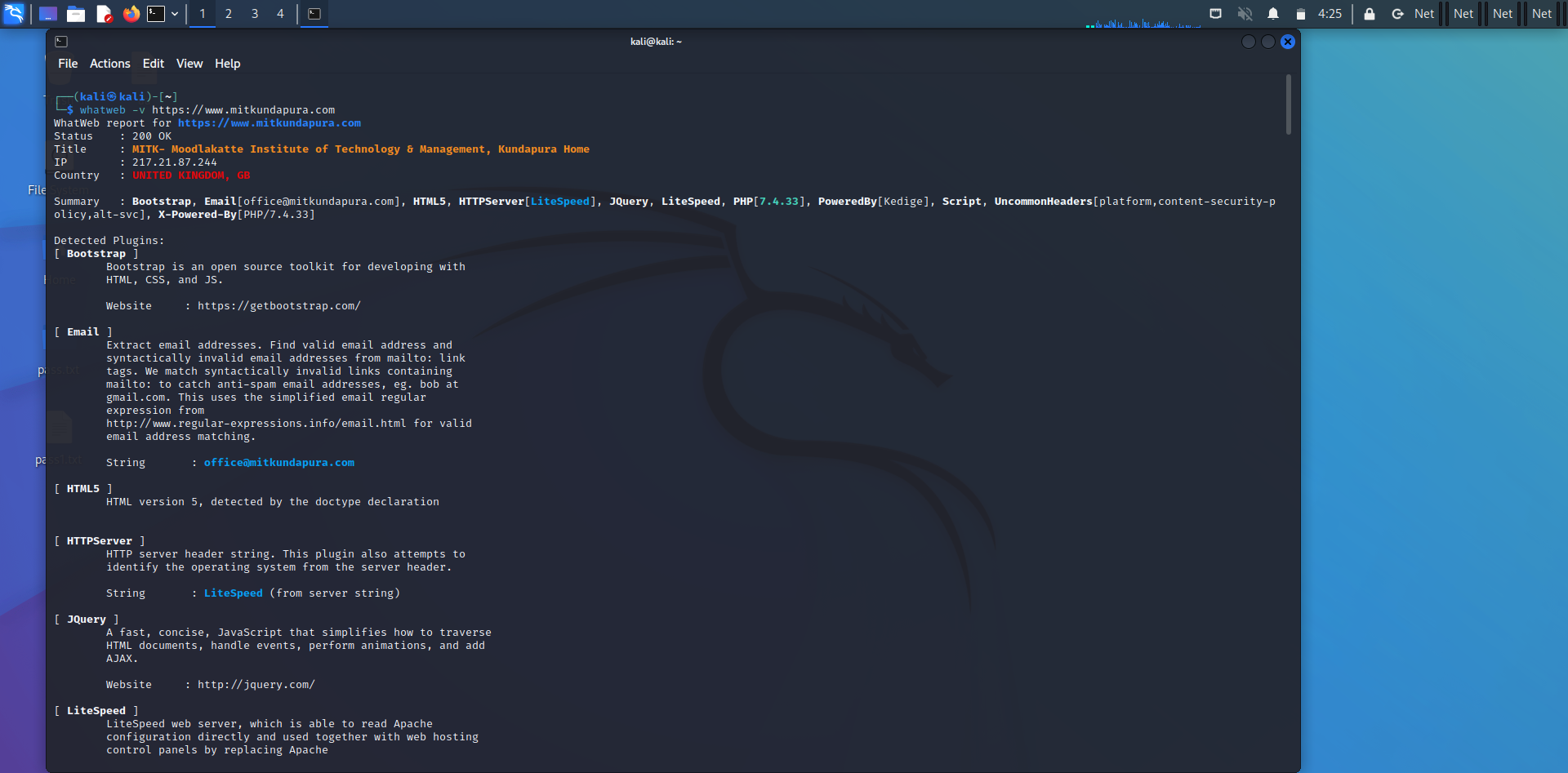
Whatweb is a scanner written in the Ruby language. This tool can identify and recognize all the web technologies available on the target website. This tool can identify technologies used by websites such as blogging, content management system, all JavaScript libraries.

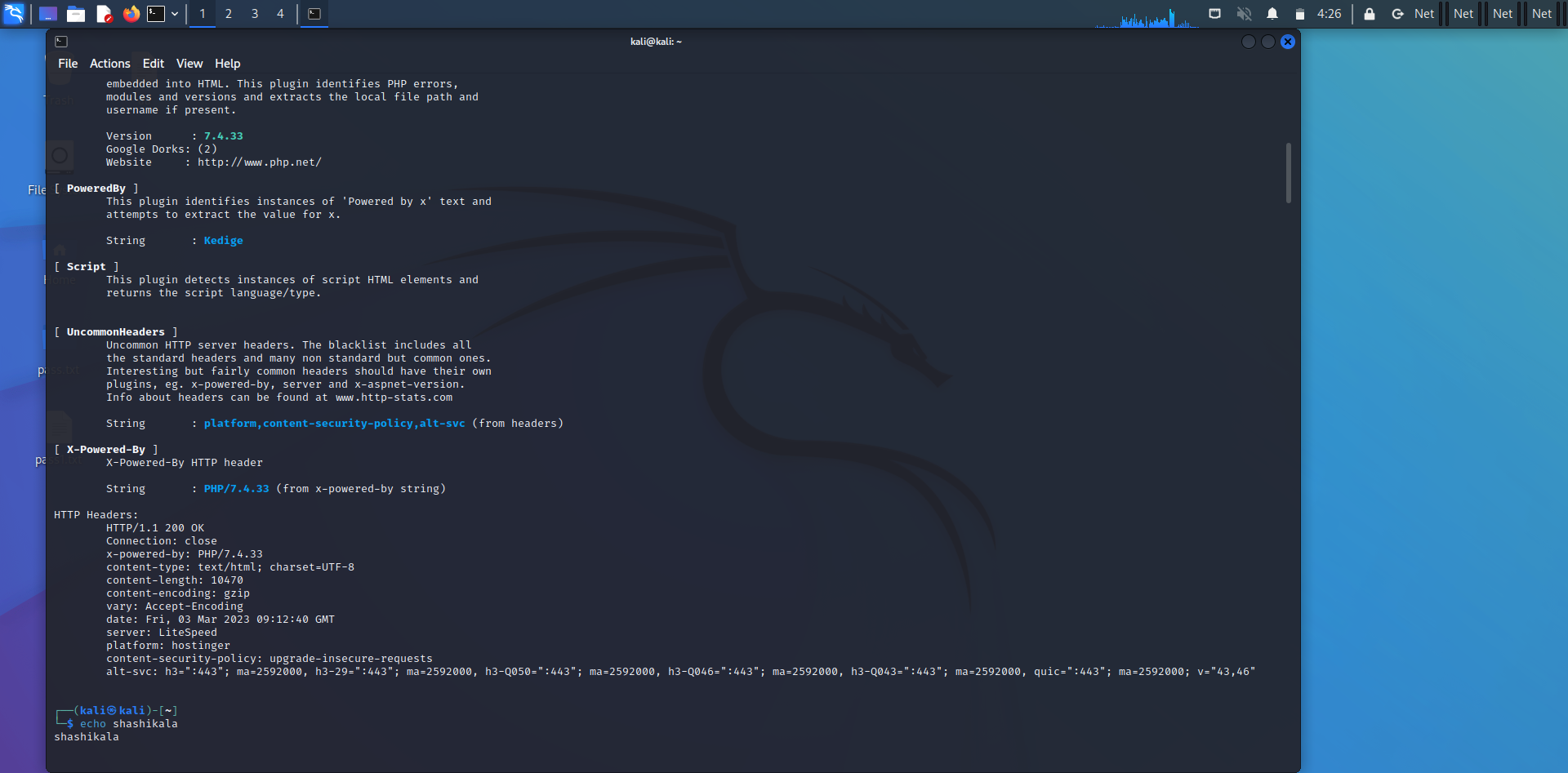
**Command:**

$ whatweb <https://www.mitkundapura.com>

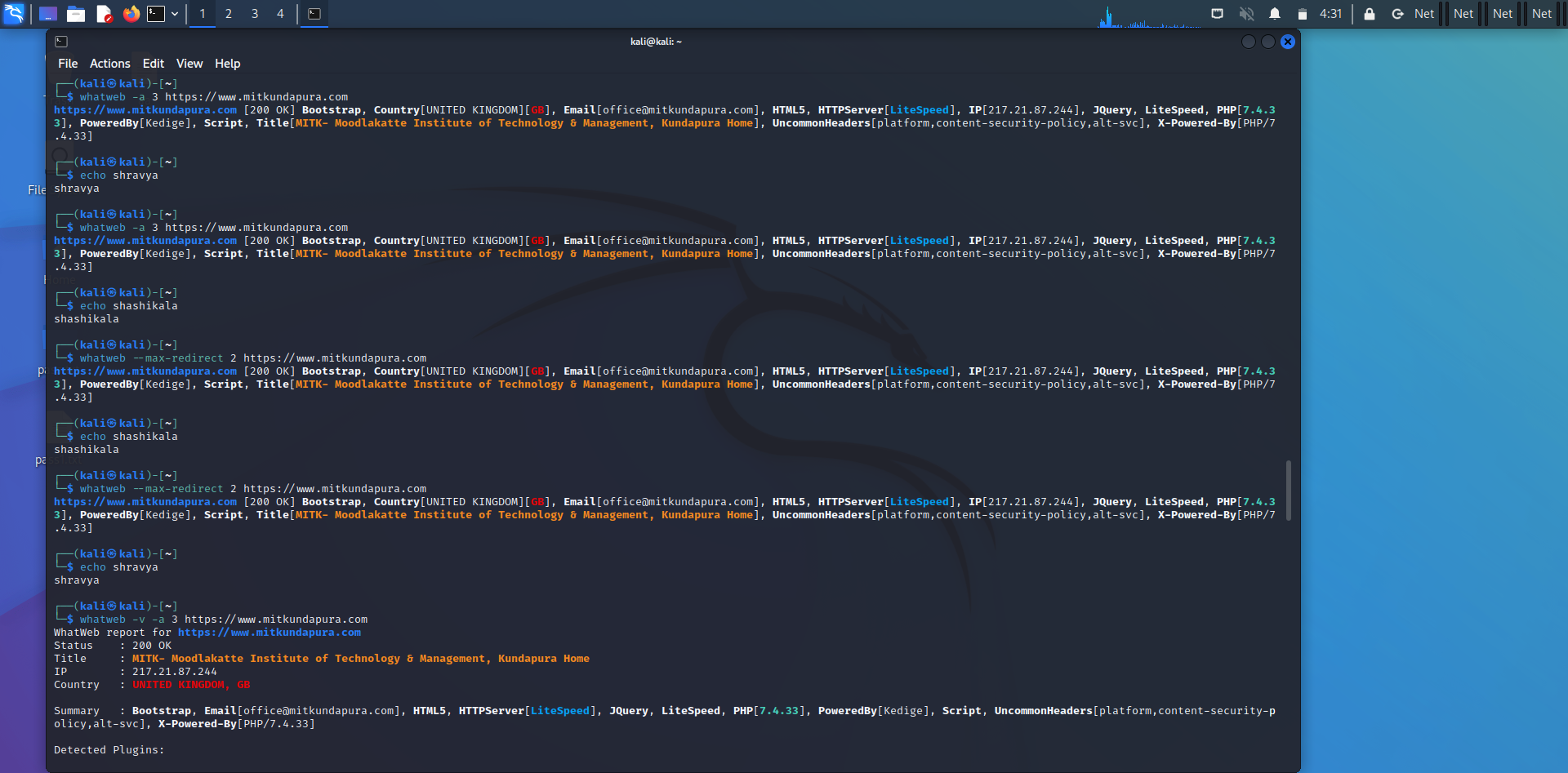


$ whatweb -v <https://www.mitkundapura.com>

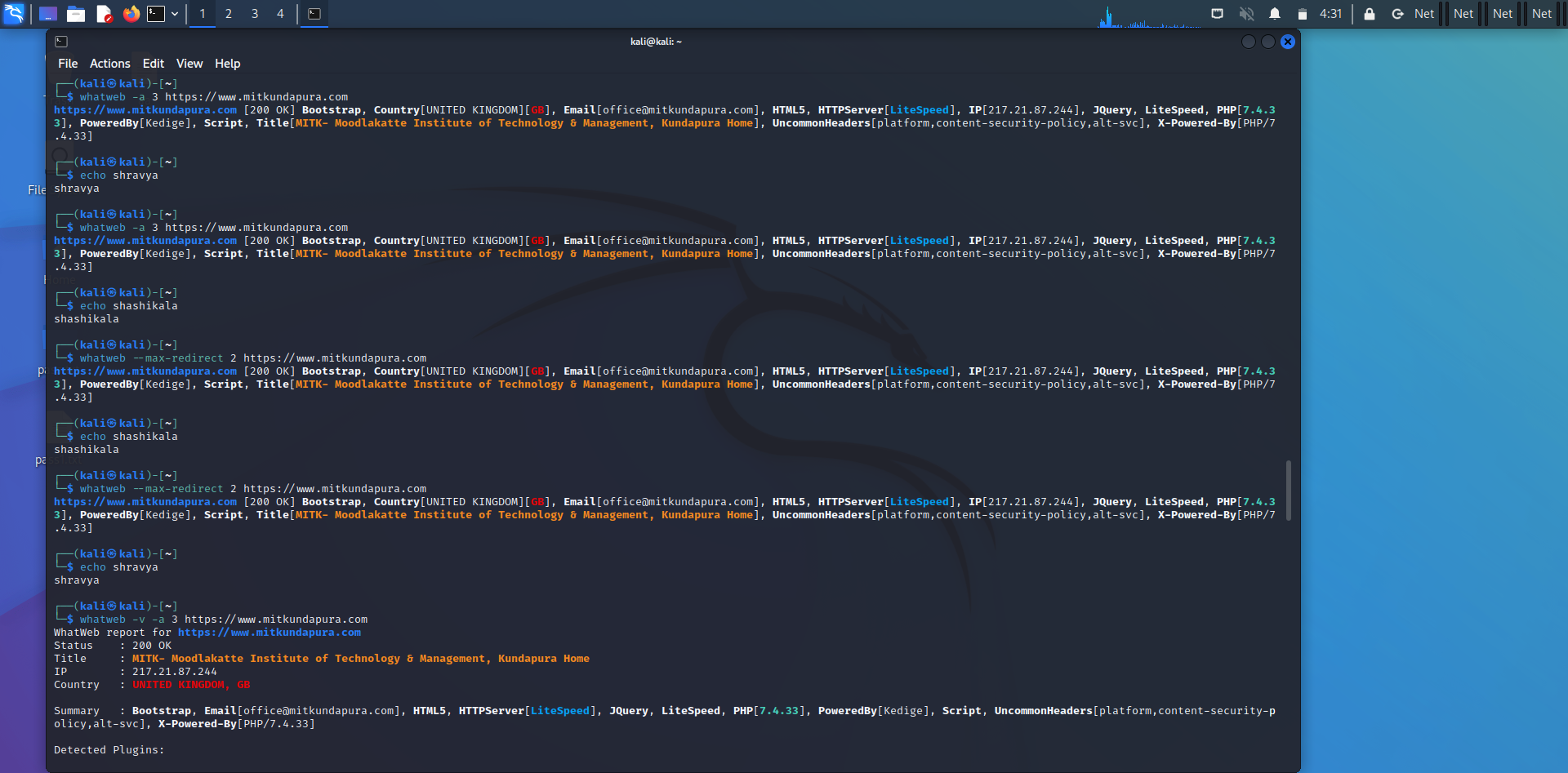




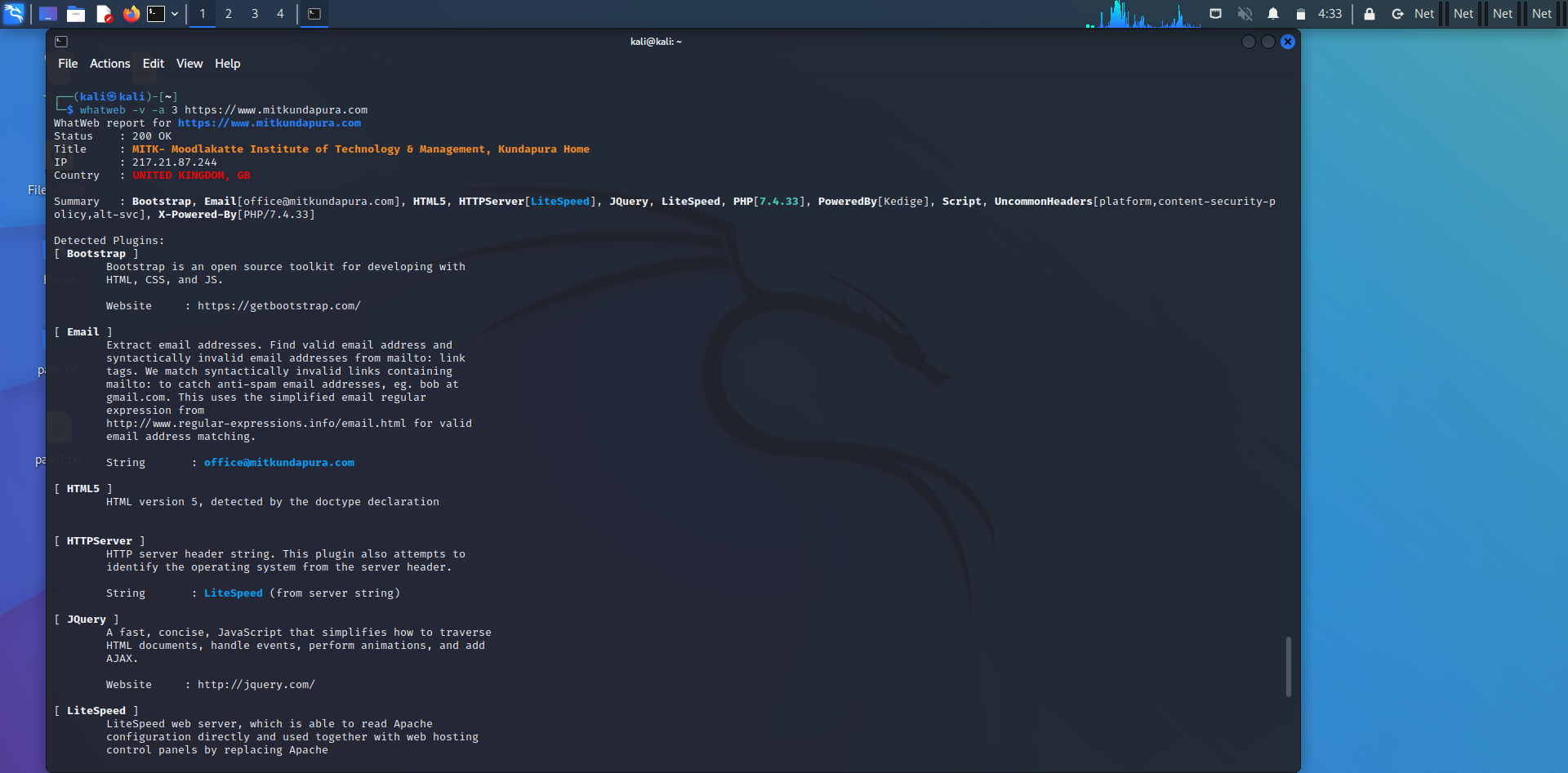
$ whatweb -a 3 <https://www.mitkundapura.com>

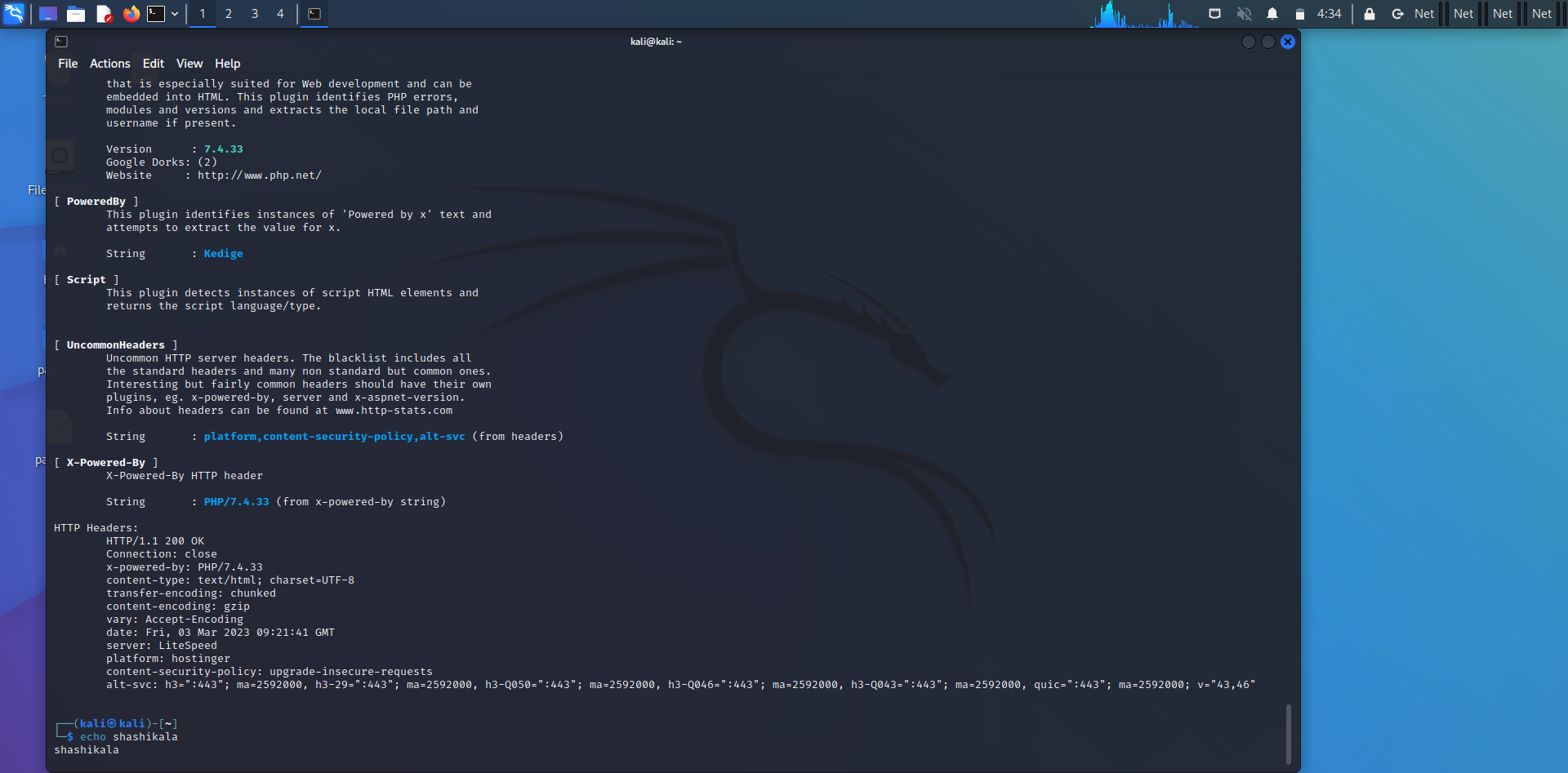


$ whatweb –max-redirect 2 <https://www.mitkundapura.com>



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



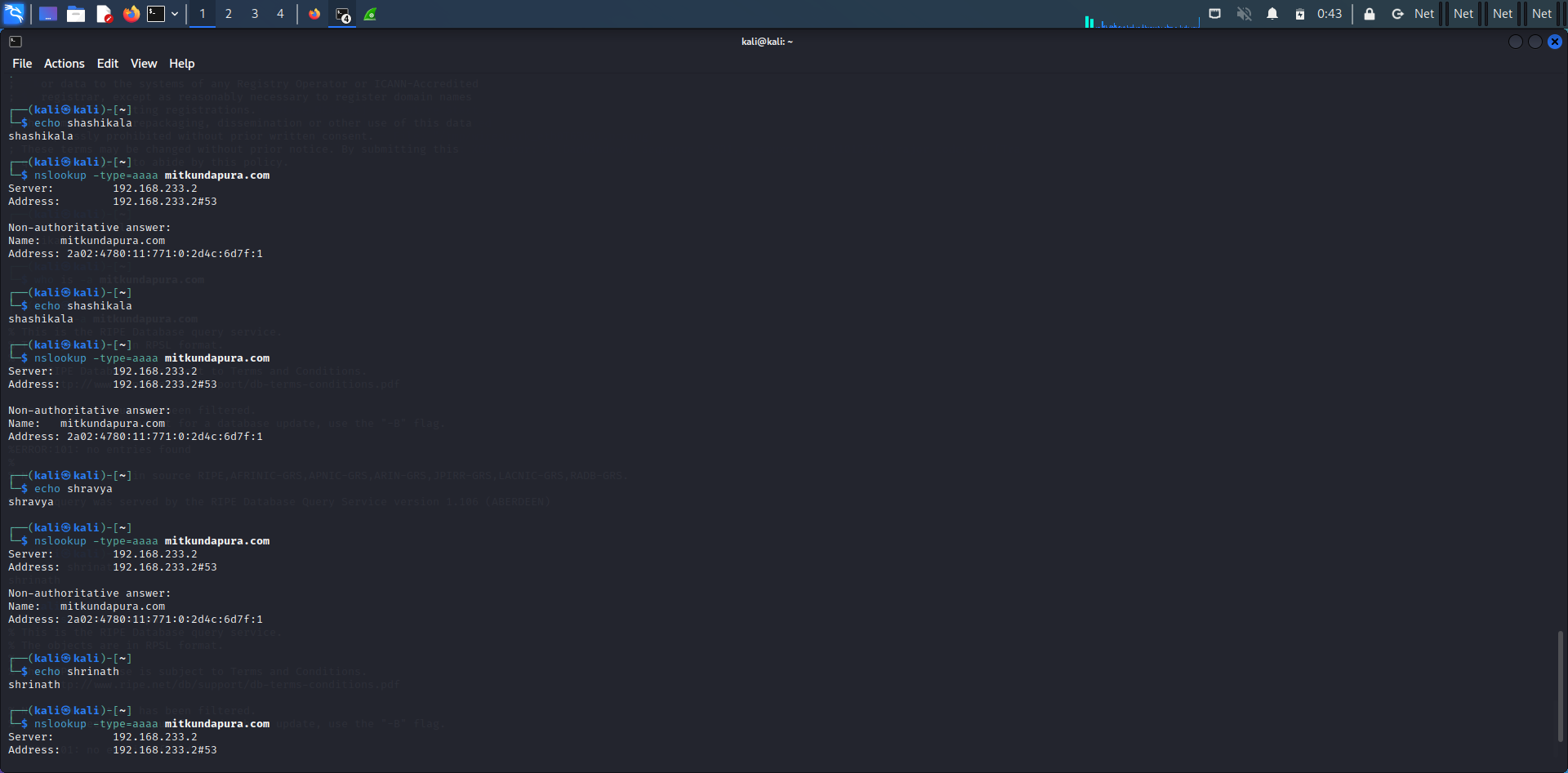


**4)Any 5 Nslookup commands:**

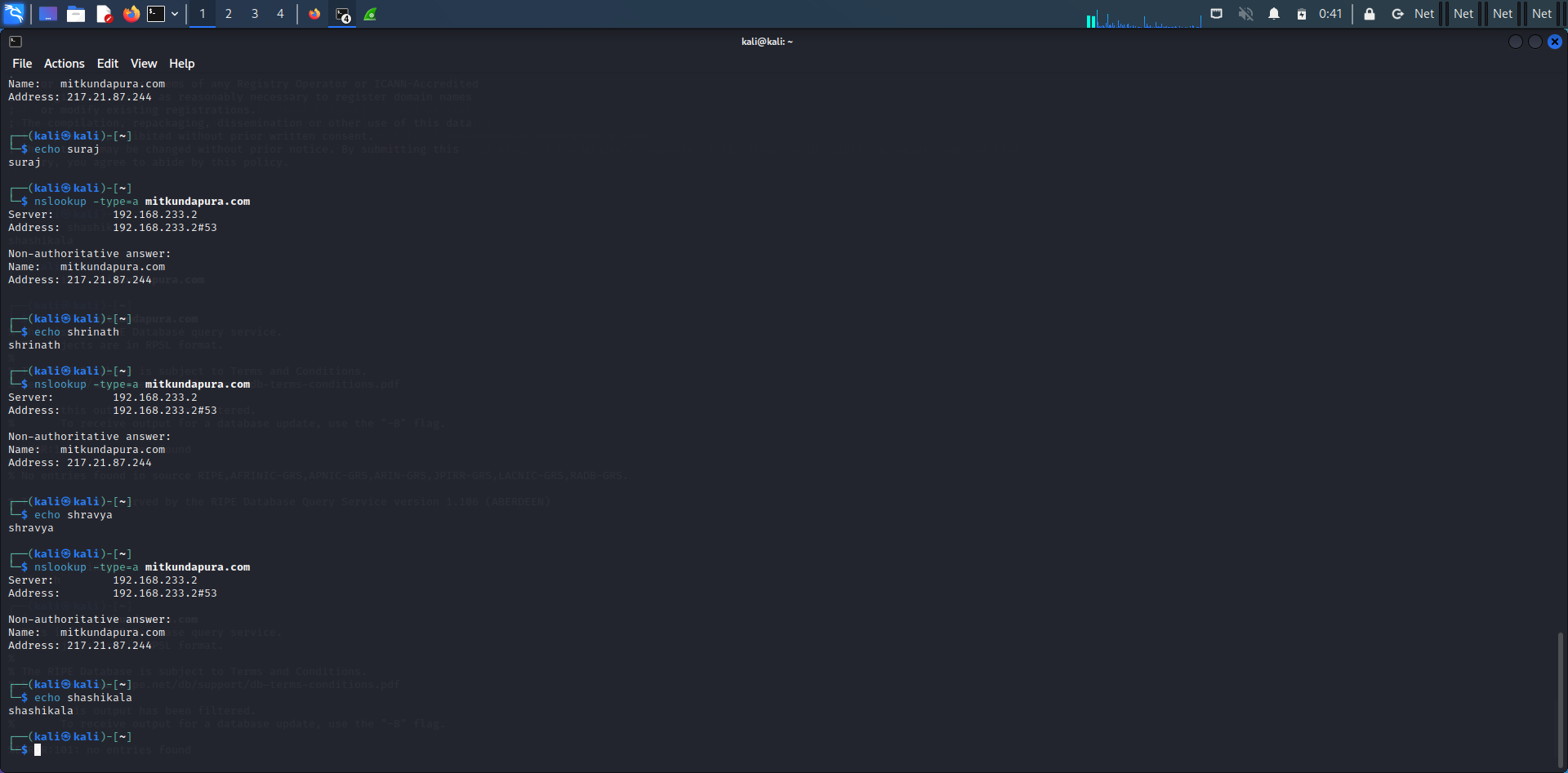
Nslookup is the name of a program that lets an Internet server administrator or any computer user enter a host name (for example, "whatis.com") and find out the corresponding IP address or domain name system (DNS) record.

**Command:**

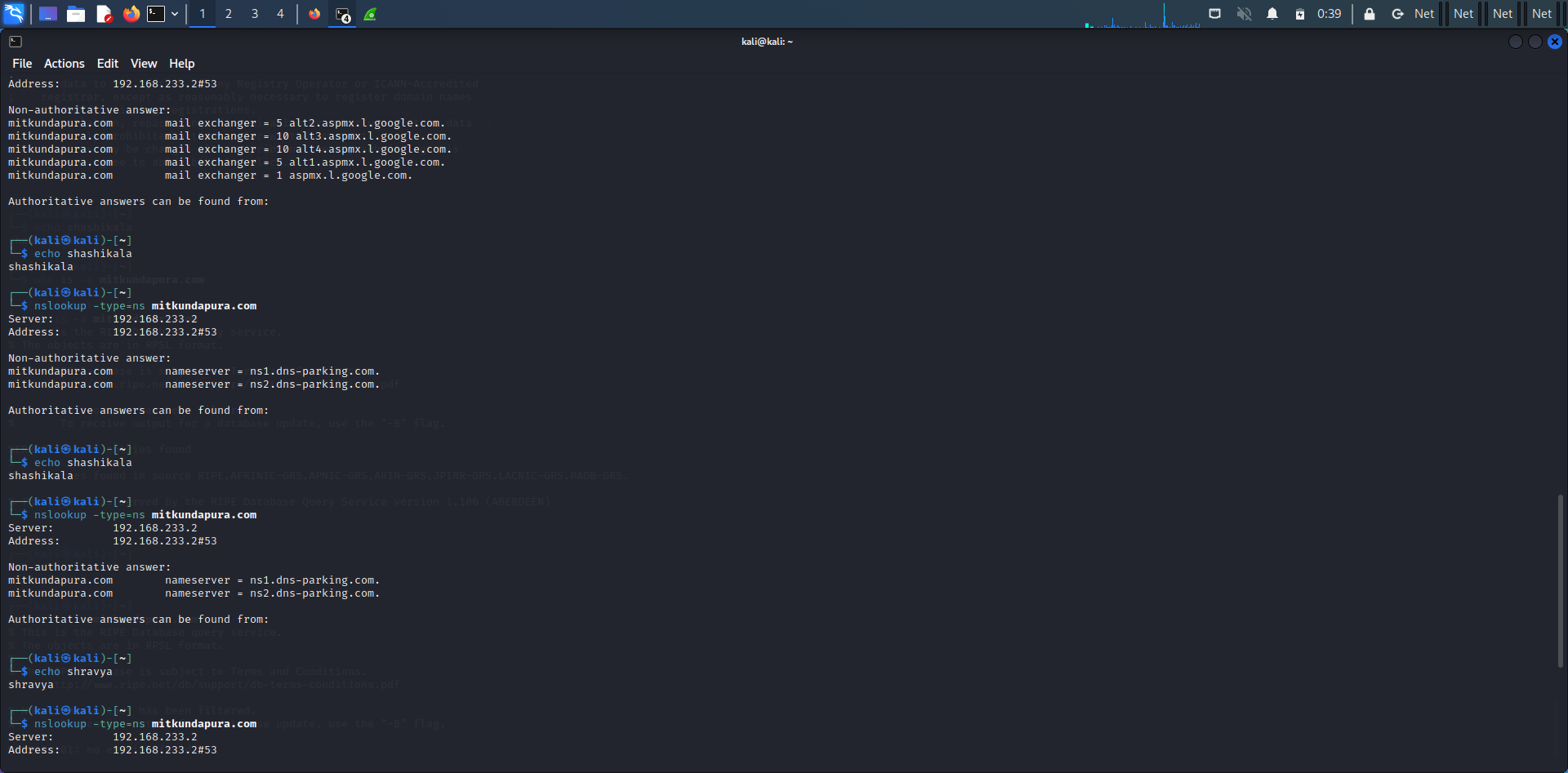
$ nslookup -type=aaaa mitkundapura.com



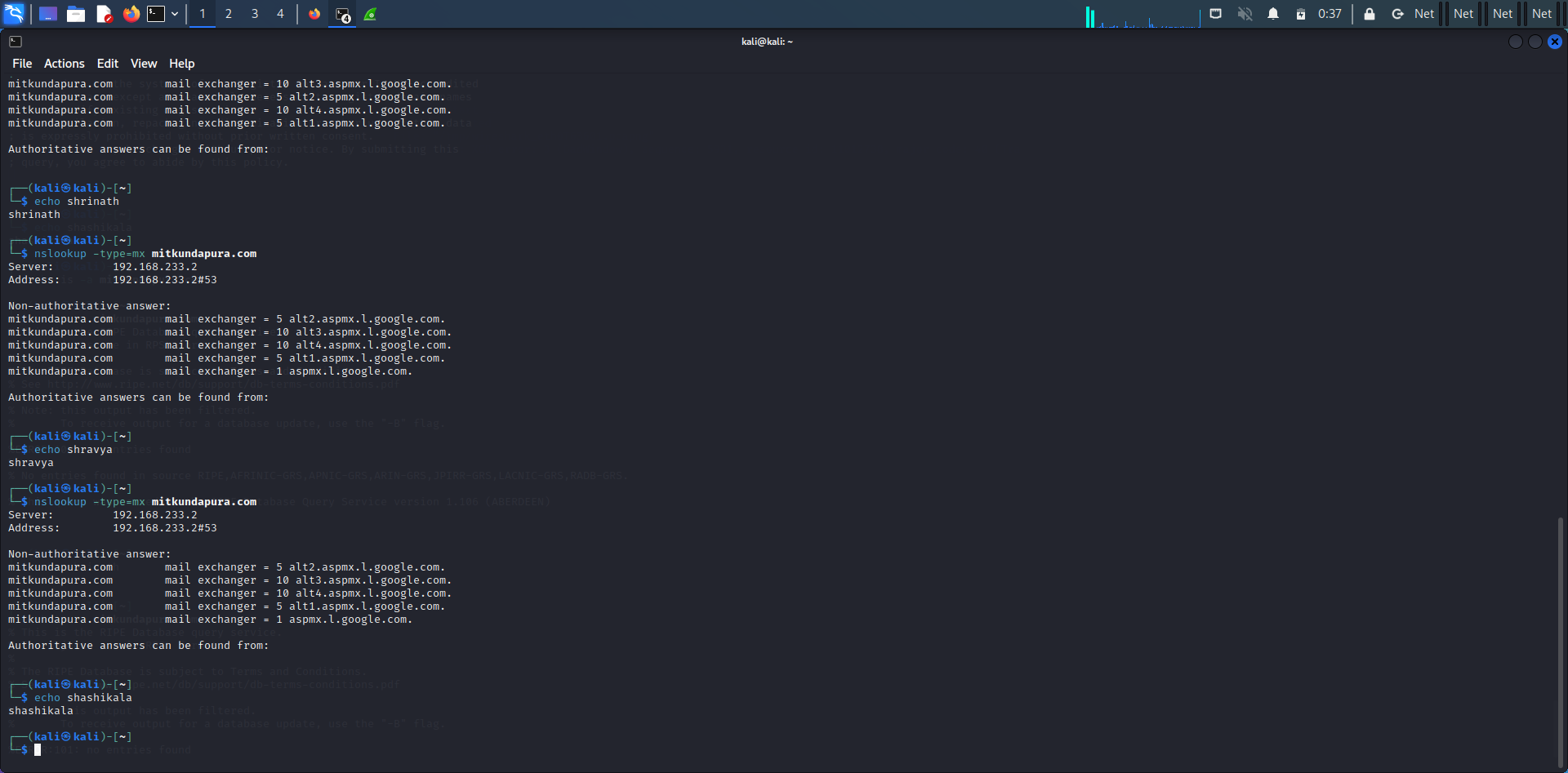
$ nslookup -type=a mitkundapura.com



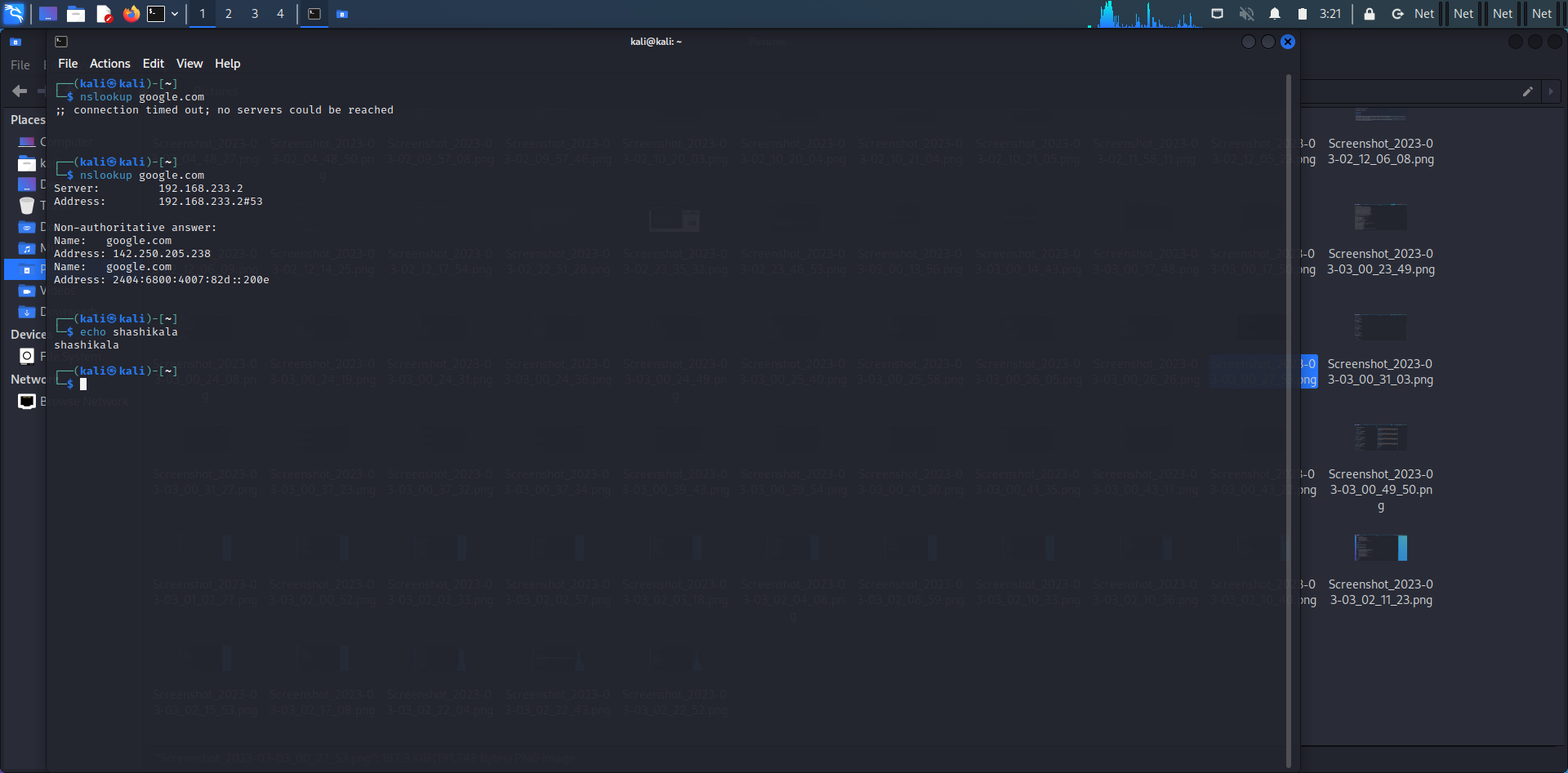
$ nslookup -type=ns mitkundapura.com



$ nslookup -type=mx mitkundapura.com



$ nslookup google.com

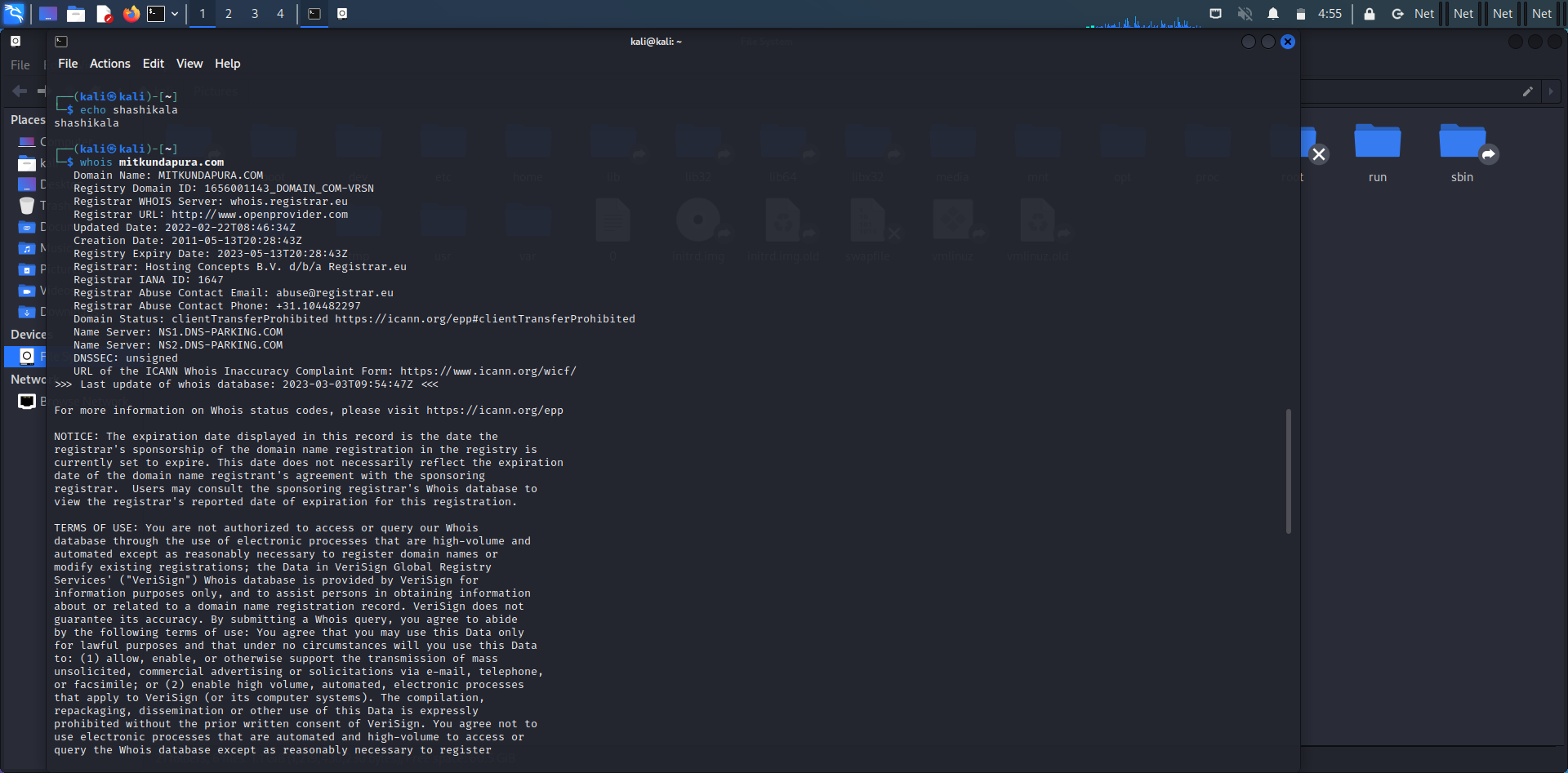


**5)Whois command:**

Whois is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them. The Internet Corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership.

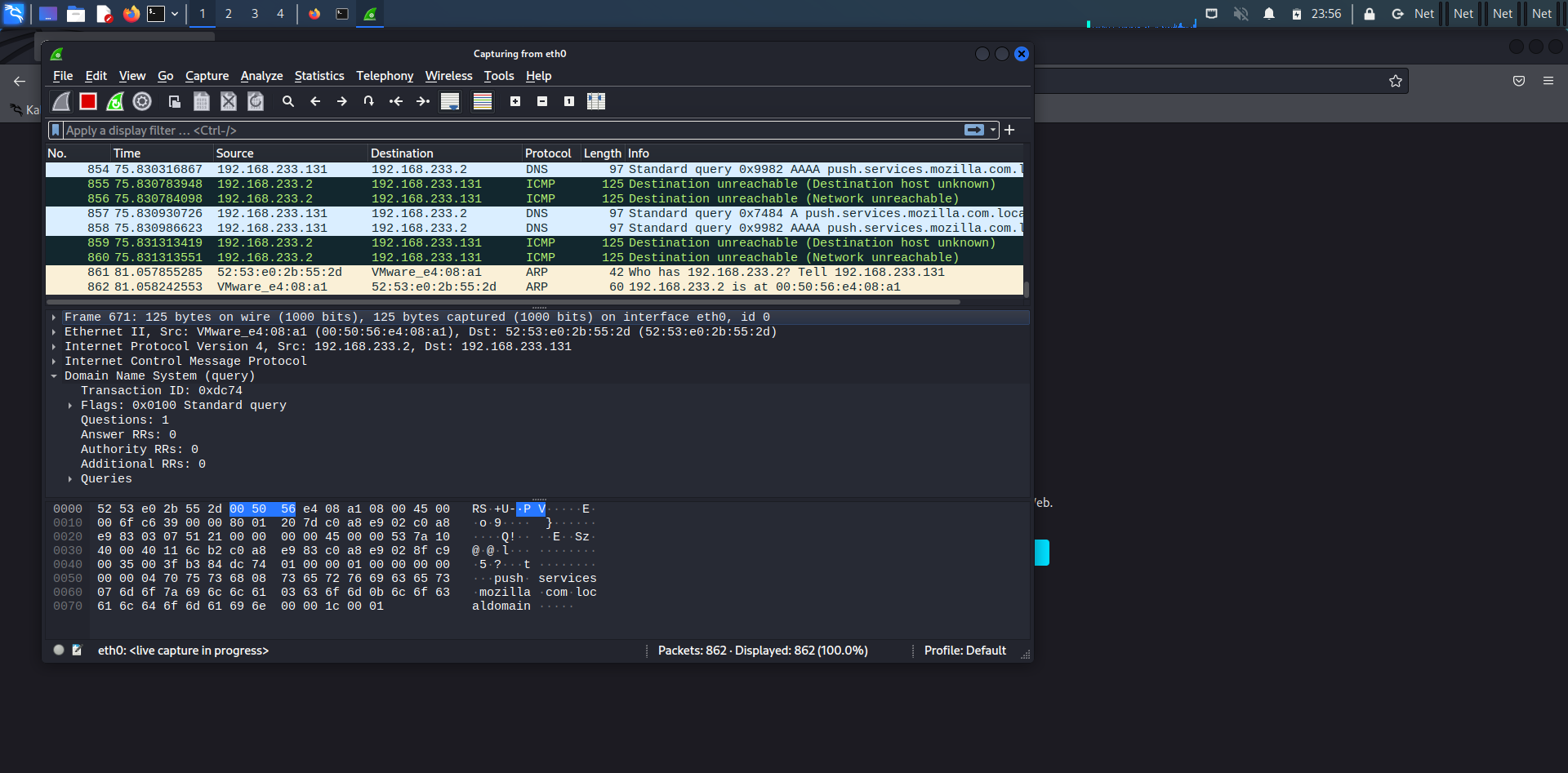
**Command:**

$ whois mitkundapura.com



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

The "Data" is a protocol that Wireshark supports, but doesn't recognize. If this is the case, you can use Wireshark's User Specified Decodes feature or its protocol preferences to force the decoding of a protocol. The "Data" is just that - the normal data payload of a protocol.

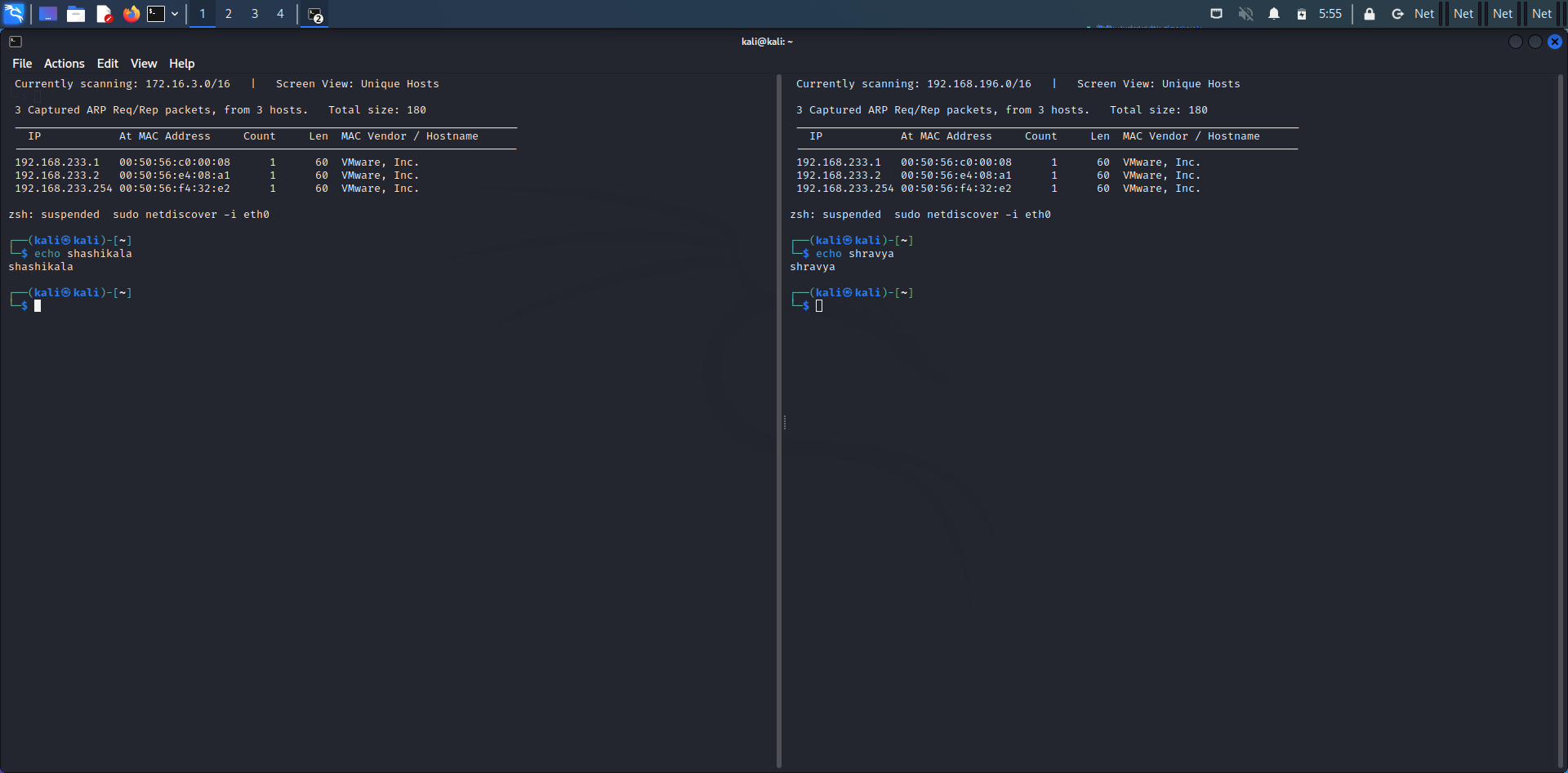


**7)Any 5 Netdiscover commands:**

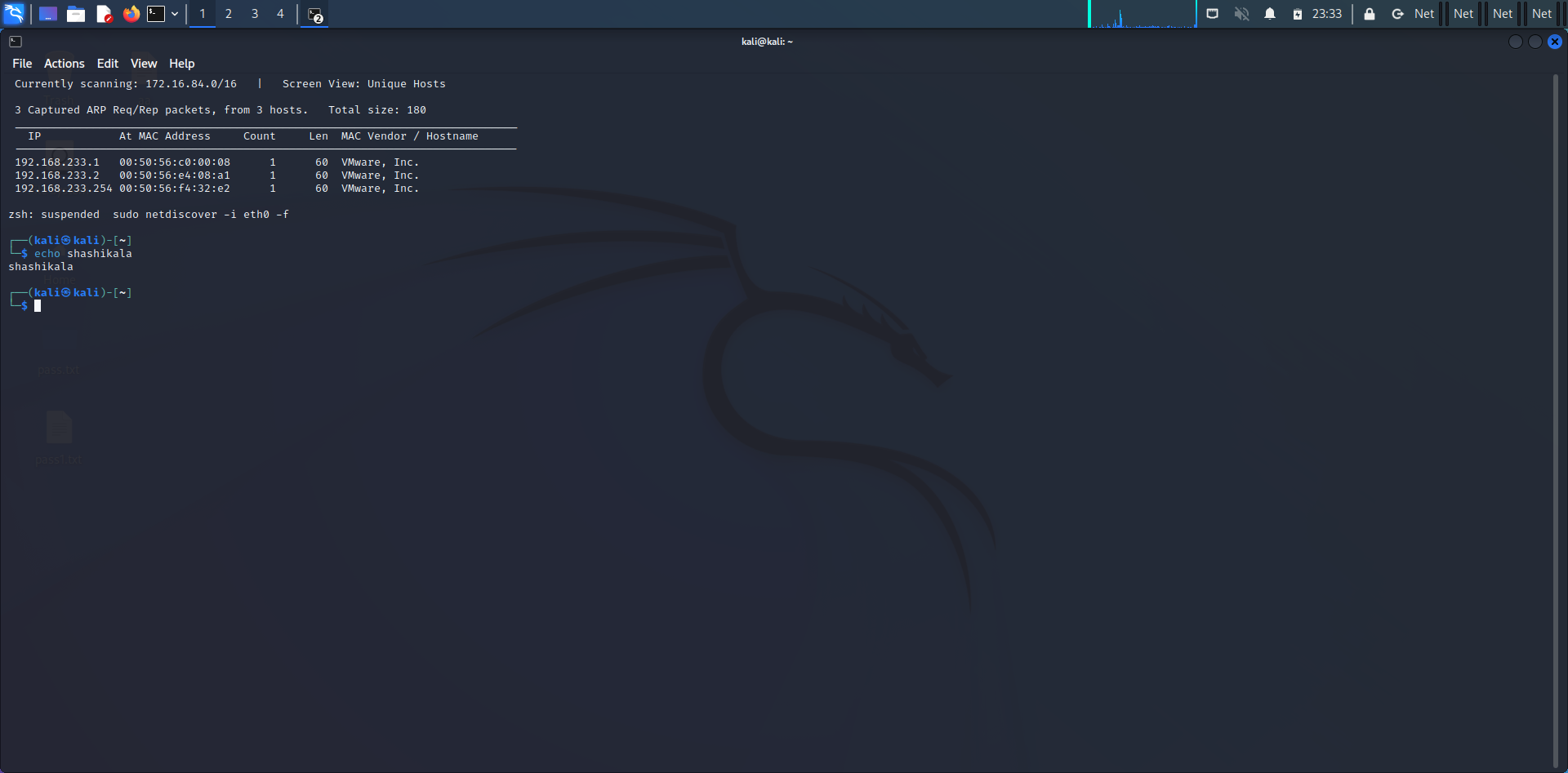
The netdiscover is a tool which is used to gather all the important information about the network. It gathers information about the connected clients and the router.

**Command:**

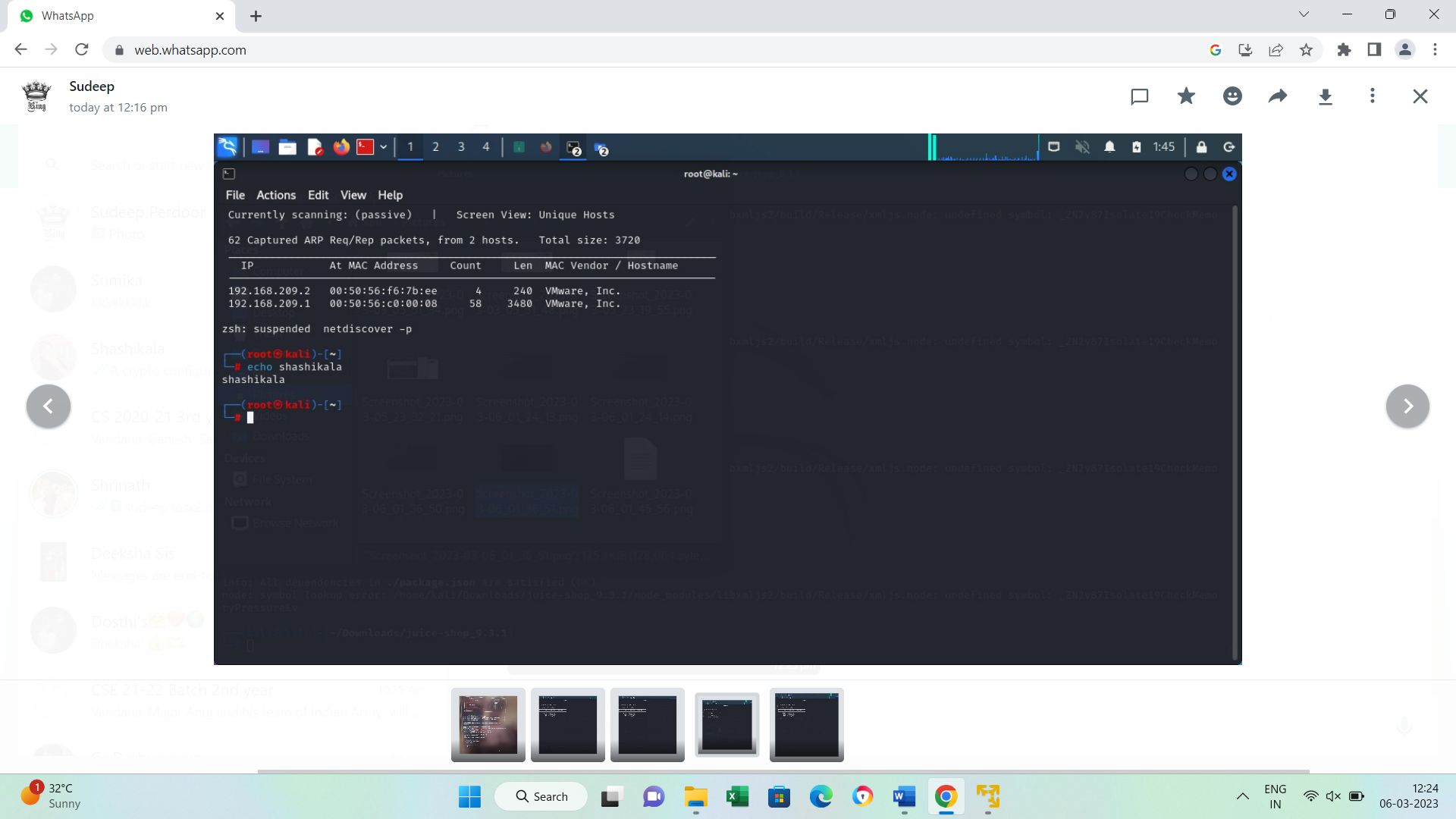
$netdiscover -i eth0



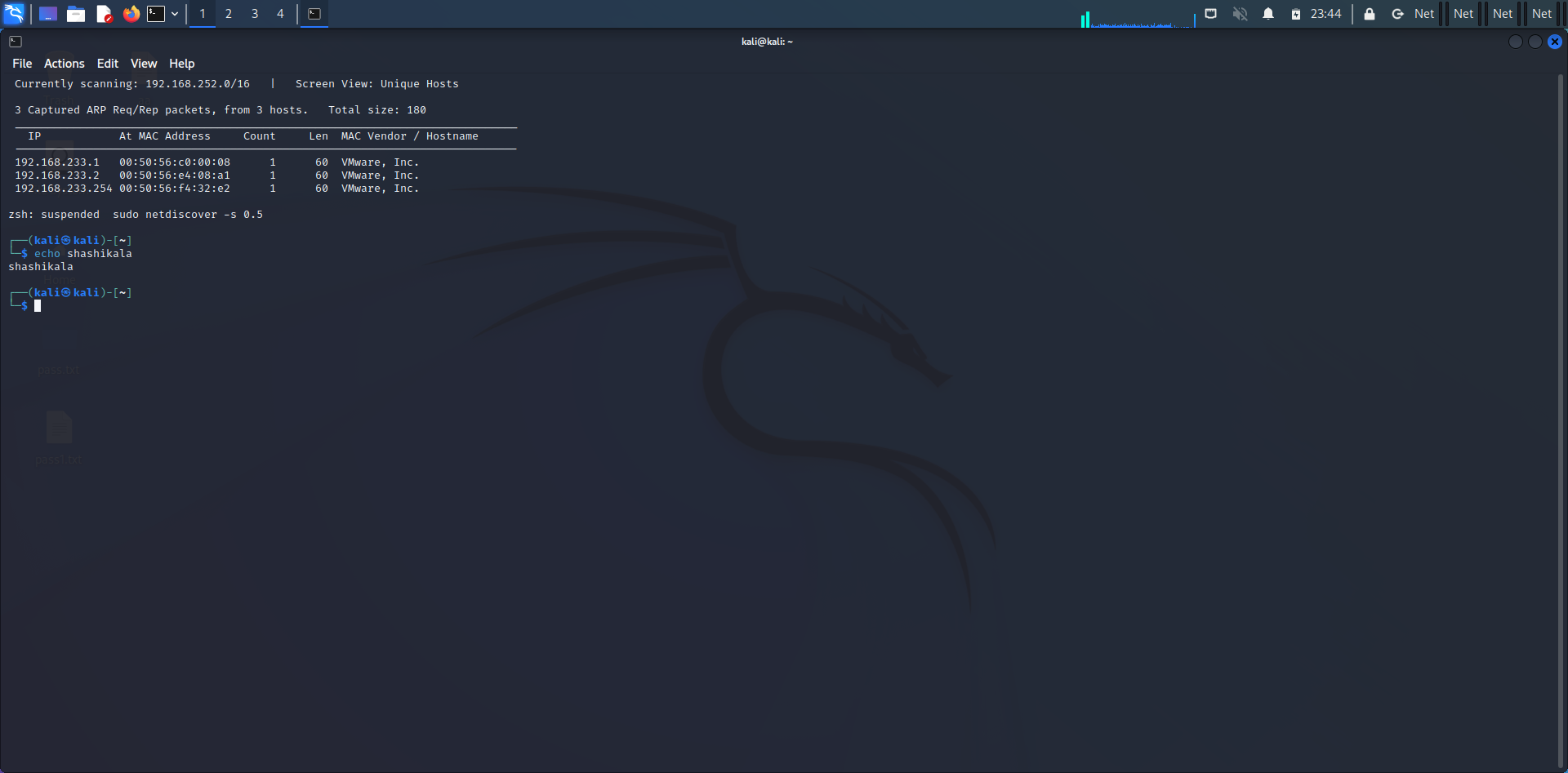
$ sudo netdiscover -i eth0 -f



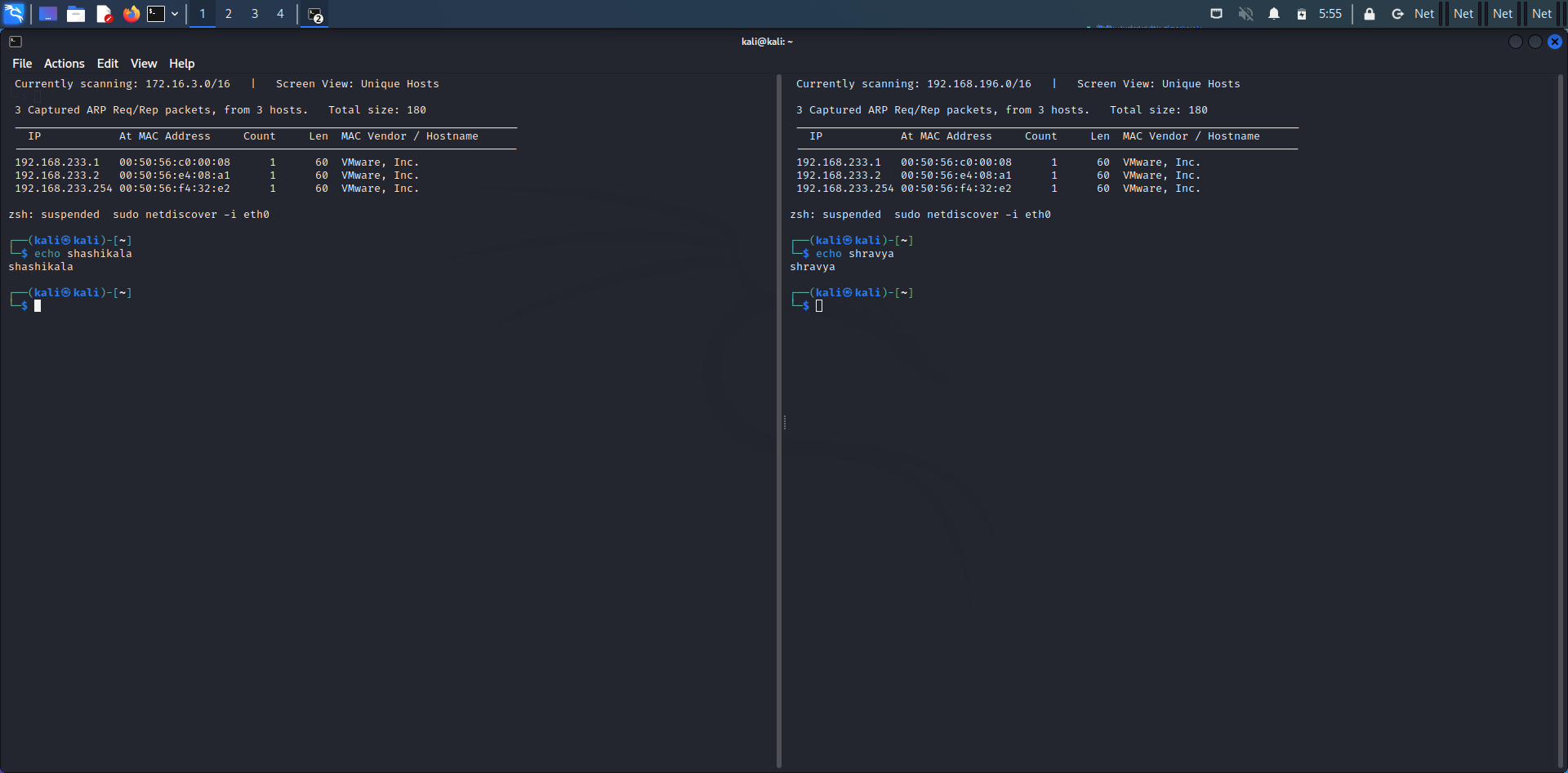
$ netdiscover -p



$ sudo netdiscover –s 0.5

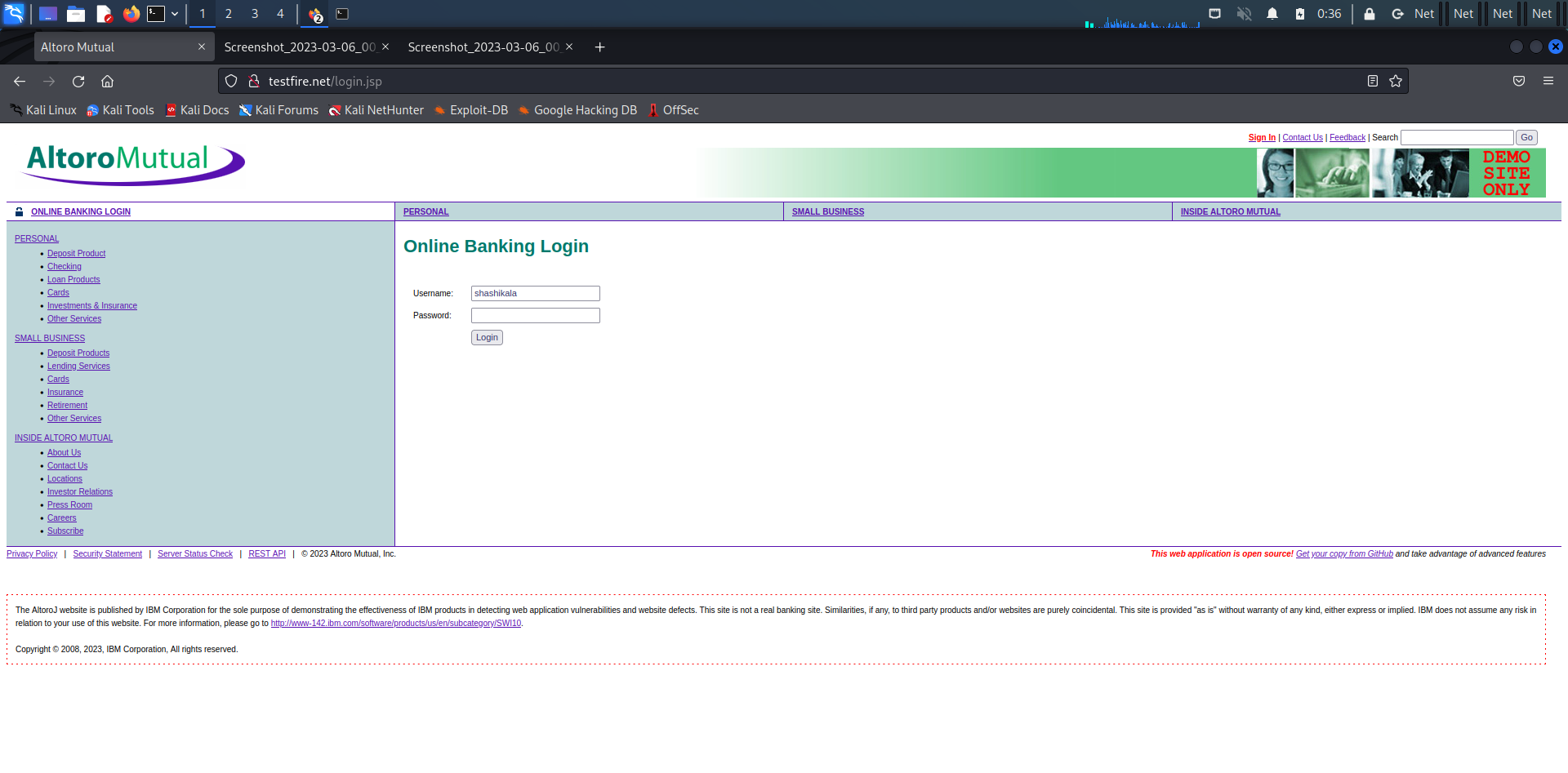


$netdiscover -i eth0



**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.

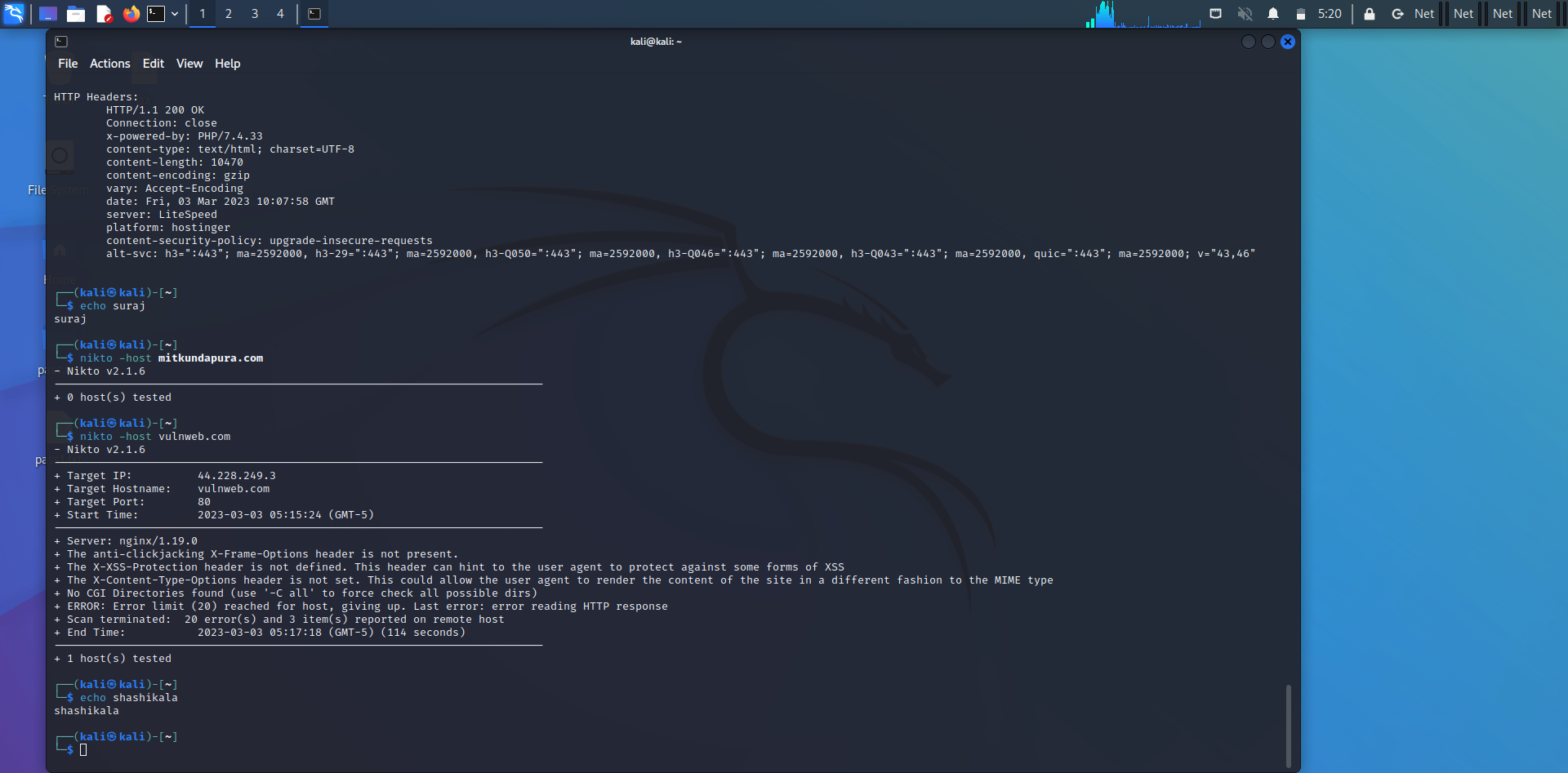


**9)Nikto commands:**

Nikto is an Open Source software written in Perl language that is used to scan a web-server for the vulnerability that can be exploited and can compromise the server. It can also check for outdated version details of 1200 server and can detect problems with specific version details of over 200 servers.

**Command:**

$ nikto –host mitkundapura.com



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

Dirbuster is a multi threaded 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. DirBuster attempts to find these.

