PROJECT 10
MAKING A BLOCKCHAIN SURVEY WITH MULTICHAIN

SPRING TRIMESTER 2022

By

NIKHIL PATEL

OVERVIEW :- In this lab, I will learn how to use multichain at the application level using PHP and multichain through API. Here I learn about a voting system in which voters receive voting tokens that they may use to vote for a certain candidate, blockchain is used for voting, and each voter can view the total number of votes cast for a candidate at any moment.

PROCEDURE :-

1) **Removing Old Multichain on the Poll Server**

   Go to one of the machine and open console and execute this command:

   ps aux | grep multi

   As a result if any Multichain daemon is running you will see on right hand side with the command line argument. Note down the id number for next step.

   For each and every multichain process execute this command to kill it:

   kill 19066(change process as per yours)

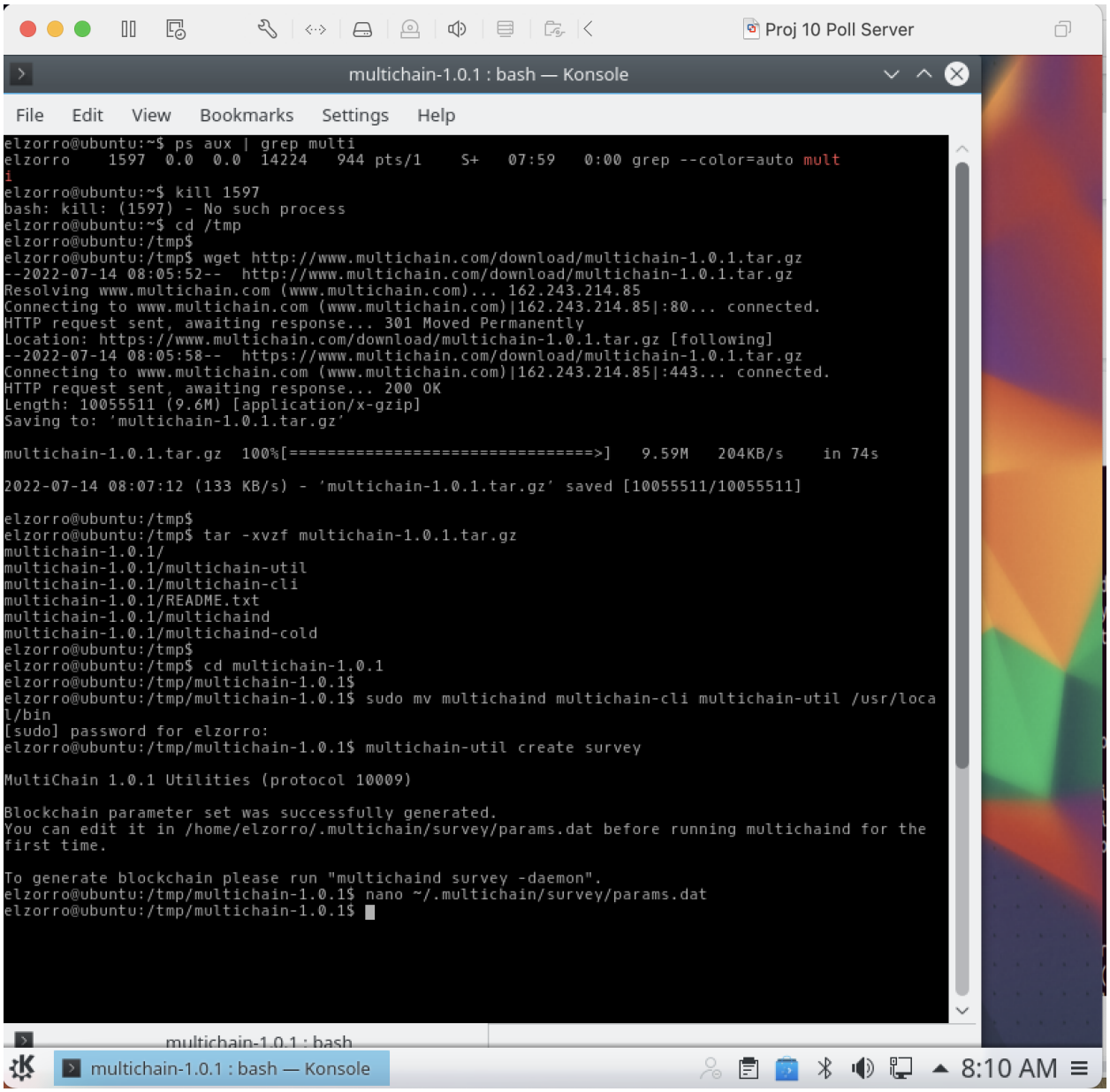
   Execute this command to remove the old multichain data form the server:

   rm -rf ~/. multichain

2) **Installing MultiChain on the Poll Server**

   To install multichain on the server follow the steps mentioned below:

   cd /tmp
   wget http://www.multichain.com/download/multichain-1.0.1.tar.gz
   tar -xvzf multichain-1.0.1.tar.gz
   cd multichain-1.0.1
   sudo mv multichaind multichain-cli multichain-util /usr/local/bin



3) Creating a Blockchain on the Poll Server

On the Poll server we will create a new blockchain named ***"Survey".***

multichain-util create survey

4) Adjusting Blockchain Settings

Go to the *poll server*, run this command:

nano ~/.multichain/survey/params.dat

Go to " *global permission* " section change these three parameter:

anyone-can-connect = true
anyone-can-send = true
anyone-can-receive = true

Go to " *Consensus requirements* " section change these three parameter:

setup-first-blocks = 10000

5) Initialize the Blockchain

Again go to poll server, run this command:

multichaind survey –daemon

The server will start and you will see the node address that others can use to connect with this string as shown below.

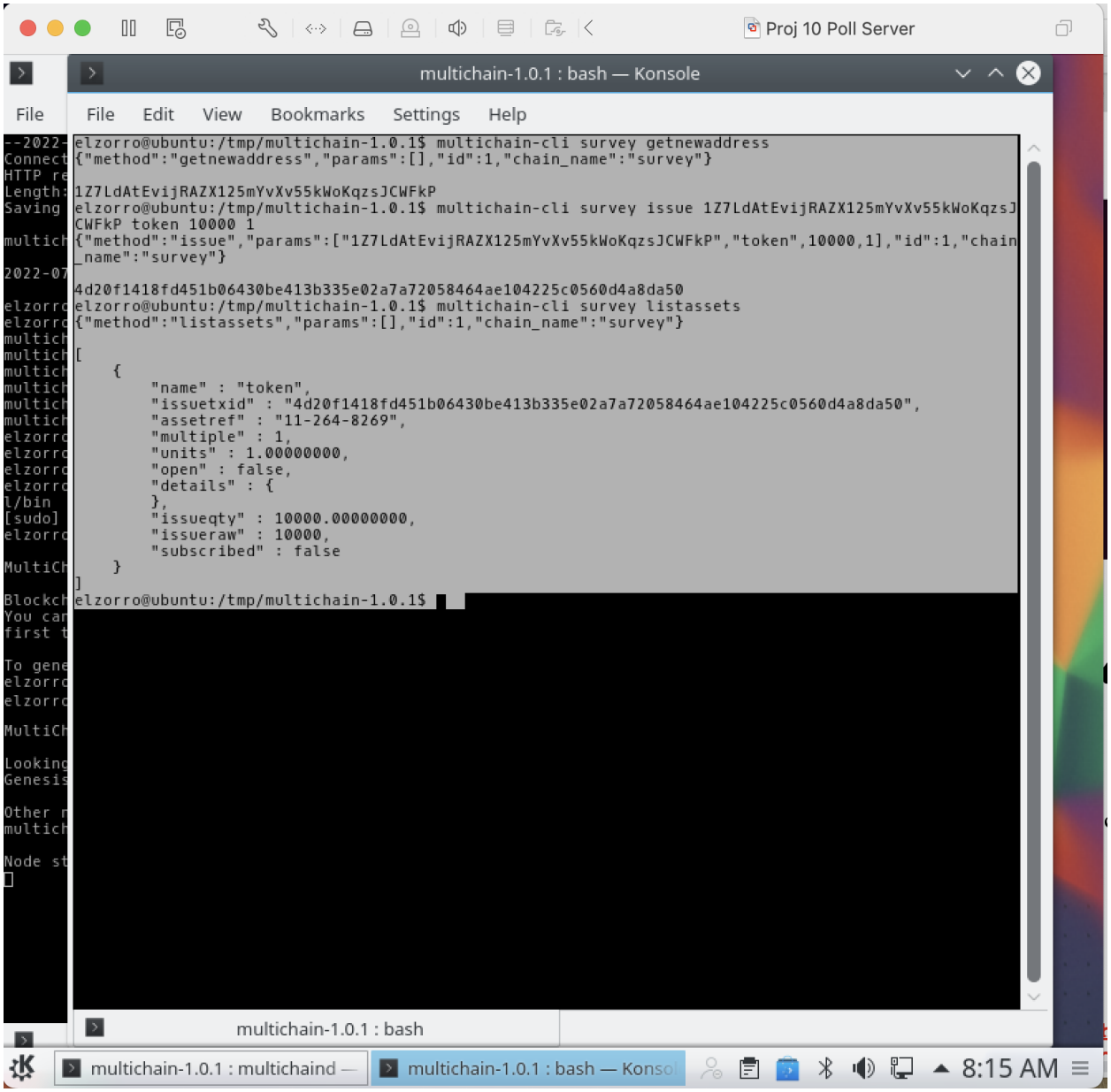
Note: ***If you didn't get a prompt after launching Node as shown in the image below, please open another console to continue with the query server commands. Minimize and do not damage the original console.***

6) Getting an Address on the Poll Server

Go to the *poll server*, run this command:

multichain-cli survey getnewaddress

Make an note of address appears as result from above command



7) Issue the "token" Asset

Now we'll build a non-subdivisible asset called "token" and place 10,000 of them on the Poll server.

multichain-cli survey issue *(Address note before)* token 10000 1

multichain-cli survey listassets

8) Install Apache on the Poll Server

Go to the *poll server*, and enter password run this command :

sudo apt-get update

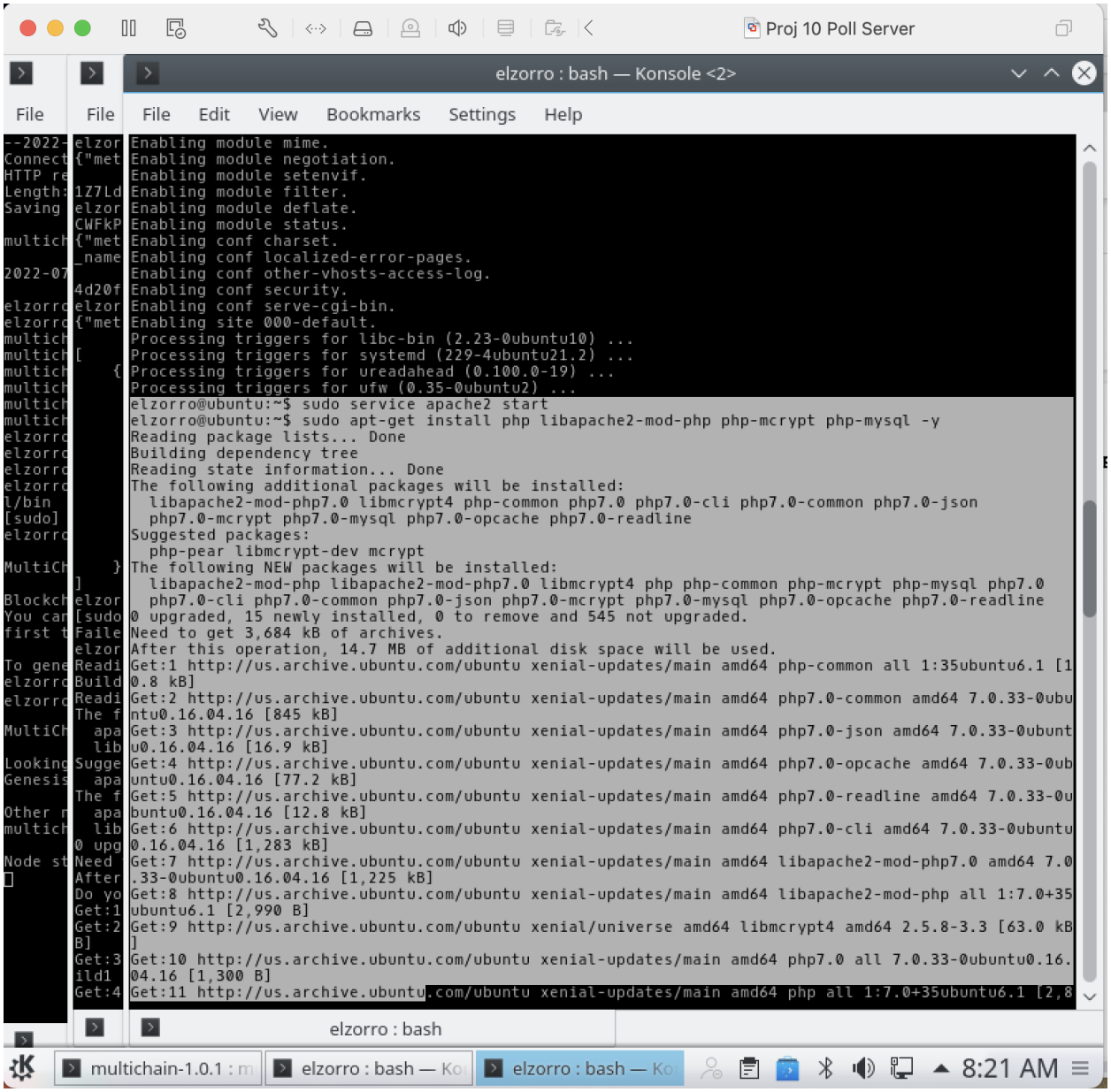
You can skip the command in red if your poll server has apache already installed.

dpkg –configure -a

sudo rm /var/cache/apt/archives/lock

sudo rm /var/lib/dpkg/lock

sudo apt-get install apache2



Then run the below command to run apache server.

sudo service apache2 start

9) Install PHP on the Poll Server

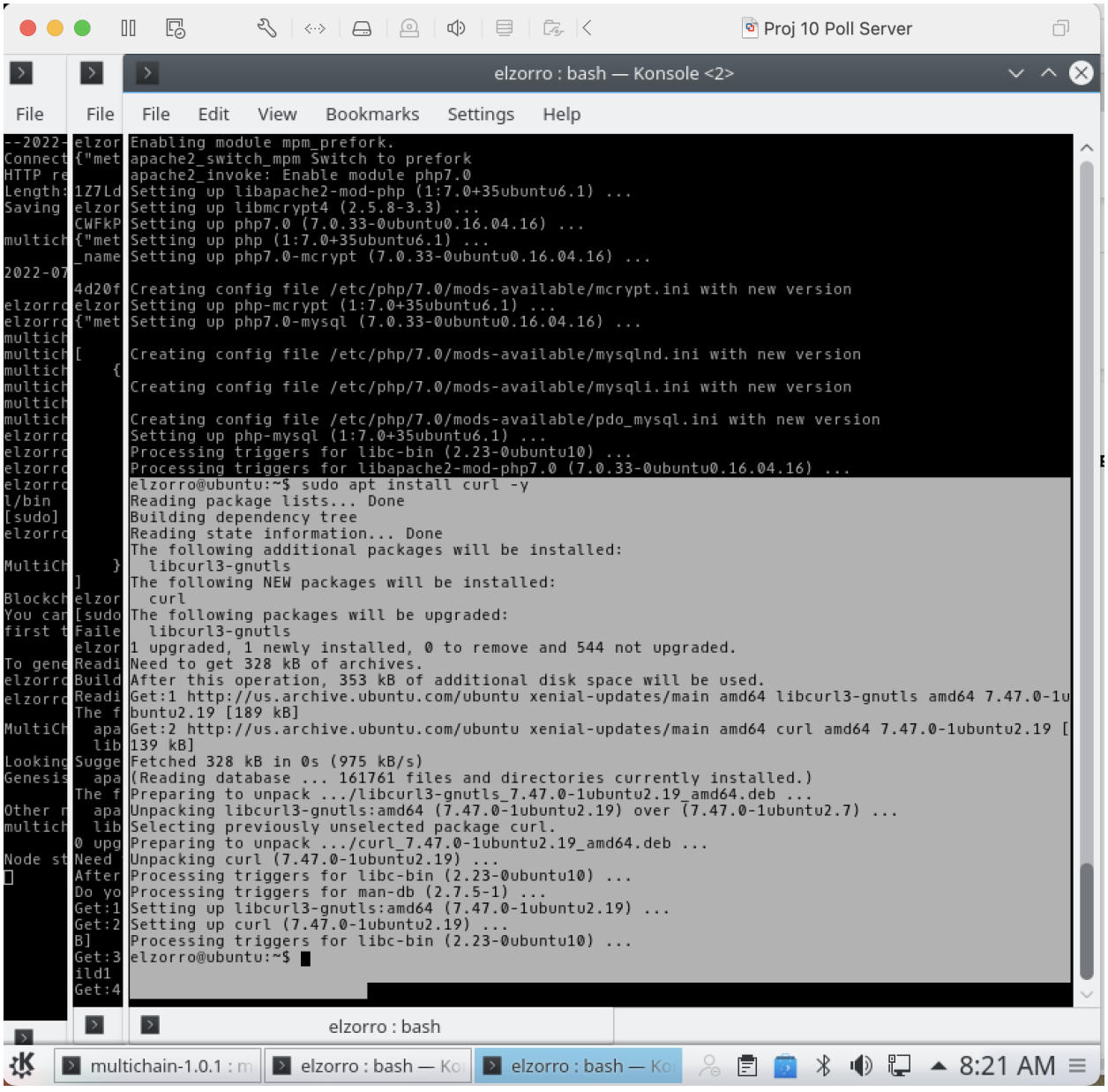
Go to the *poll server*, run this command:

sudo apt-get install php libapache2-mod-php php-mcrypt php-mysql -y

10) Install Curl on the Poll Server

Go to the *poll server*, run this command:

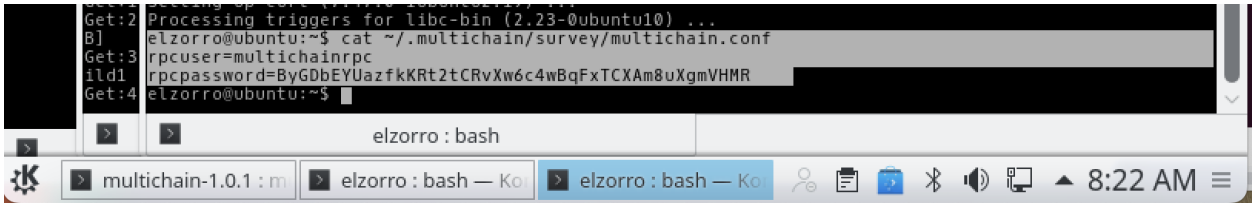
sudo apt install curl -y



11) Find your RPC Credentials

Go to the *poll server*, run this command:

cat ~/.multichain/survey/multichain.conf

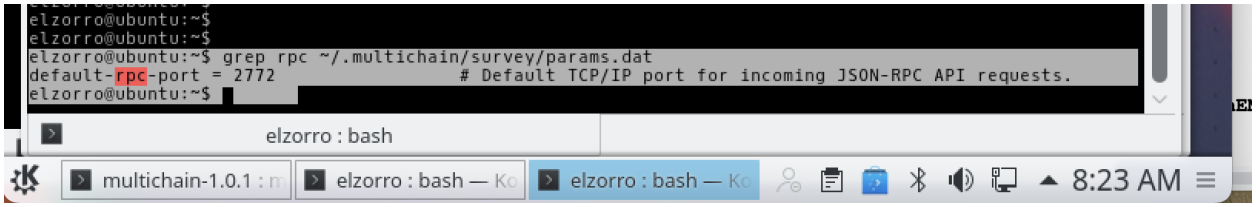


After executing the above command you will get username & password for RPC.

12) Find your RPC Port

Go to the *poll server*, run this command:

grep rpc ~/.multichain/survey/params.dat



13) Make the info.php Script

Go to the *poll server*, run this command:

sudo nano /var/www/html/info.php

Enter or paste in this code. You will need to change two items:

1. Replace the password in the line beginning with "$a" with the correct password on your Poll Server
2. Replace the port number at the end of the line beginning with "$c" with the actual port number on your server.

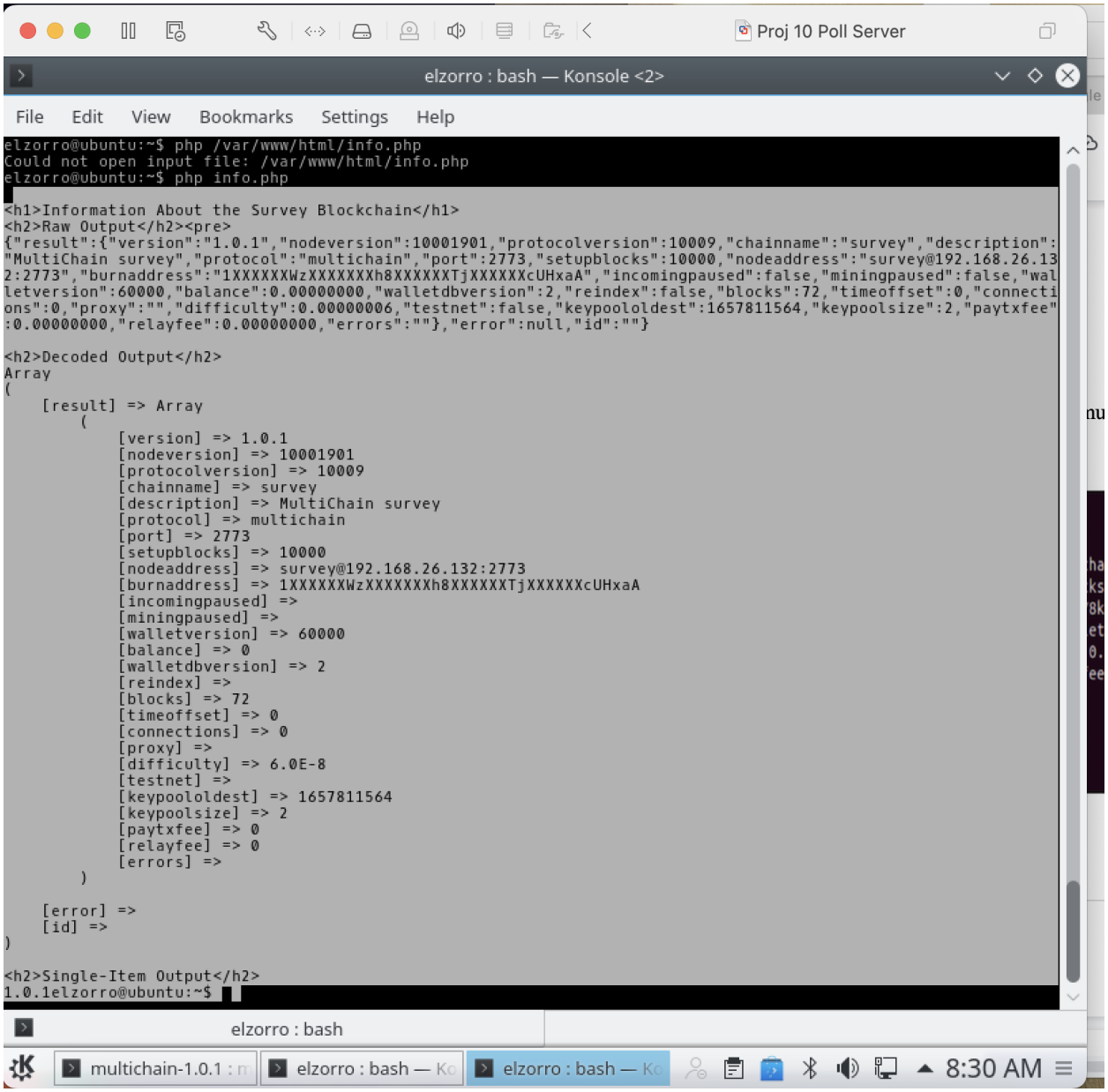
<?php
echo "<h1>Information About the Survey Blockchain</h1>";

$a = 'curl -s --user multichainrpc:8EC2qNiyoyAVj6dQE6Sf5VuyVJF2zSewrsixnEMdoh7t --data-binary \";
$b = '{"jsonrpc": "1.0", "id":"", "method": "getinfo", "params": [';
$c = '] }\' -H "content-type: text/plain;" http://127.0.0.1:9706/';
$cmd = $a . $b . $c;

```
echo "\n<h2>Raw Output</h2><pre>\n";
$ret=system($cmd);

echo "\n<h2>Decoded Output</h2>\n";
$rets = json_decode($ret, true);
print_r($rets);

echo "\n<h2>Single-Item Output</h2>\n";
echo $rets['result']['version'];
?>
```

14) **Testing the info.php Script**

```
php /var/www/html/info.php
```


Proj 10 Poll Server
elzorro : bash — Konsole <2>
File Edit View Bookmarks Settings Help
elzorro@ubuntu:~$ php /var/www/html/info.php
Could not open input file: /var/www/html/info.php
elzorro@ubuntu:~$ php info.php
<h1>Information About the Survey Blockchain</h1>
<h2>Raw Output</h2><pre>
{"result":{"version":"1.0.1","nodeversion":10001901,"protocolversion":10009,"chainname":"survey","description":
"MultiChain survey","protocol":"multichain","port":2773,"setupblocks":10000,"nodeaddress":"survey@192.168.26.13
2:2773","burnaddress":"1XXXXXXWzXXXXXXXh8XXXXXXTjXXXXXXcUHxaA","incomingpaused":false,"miningpaused":false,"wal
letversion":60000,"balance":0.00000000,"walletdbversion":2,"reindex":false,"blocks":72,"timeoffset":0,"connecti
ons":0,"proxy":"","difficulty":0.00000006,"testnet":false,"keypoololdest":1657811564,"keypoolsize":2,"paytxfee"
:0.00000000,"relayfee":0.00000000,"errors":""},"error":null,"id":""}
<h2>Decoded Output</h2>
Array
(
[result] => Array
(
[version] => 1.0.1
[nodeversion] => 10001901
[protocolversion] => 10009
[chainname] => survey
[description] => MultiChain survey
[protocol] => multichain
[port] => 2773
[setupblocks] => 10000
[nodeaddress] => survey@192.168.26.132:2773
[burnaddress] => 1XXXXXXWzXXXXXXXh8XXXXXXTjXXXXXXcUHxaA
[incomingpaused] =>
[miningpaused] =>
[walletversion] => 60000
[balance] => 0
[walletdbversion] => 2
[reindex] =>
[blocks] => 72
[timeoffset] => 0
[connections] => 0
[proxy] =>
[difficulty] => 6.0E-8
[testnet] =>
[keypoololdest] => 1657811564
[keypoolsize] => 2
[paytxfee] => 0
[relayfee] => 0
[errors] =>
)
[error] =>
[id] =>
)
<h2>Single-Item Output</h2>
1.0.1elzorro@ubuntu:~$
elzorro : bash
multichain-1.0.1 : m
elzorro : bash — Ko
elzorro : bash — Ko
8:30 AM

15) Make a pay.php Script

You may create a script that pays out a token now that you know how to operate the Multichain from PHP. The script will deliver a single token to a given address.

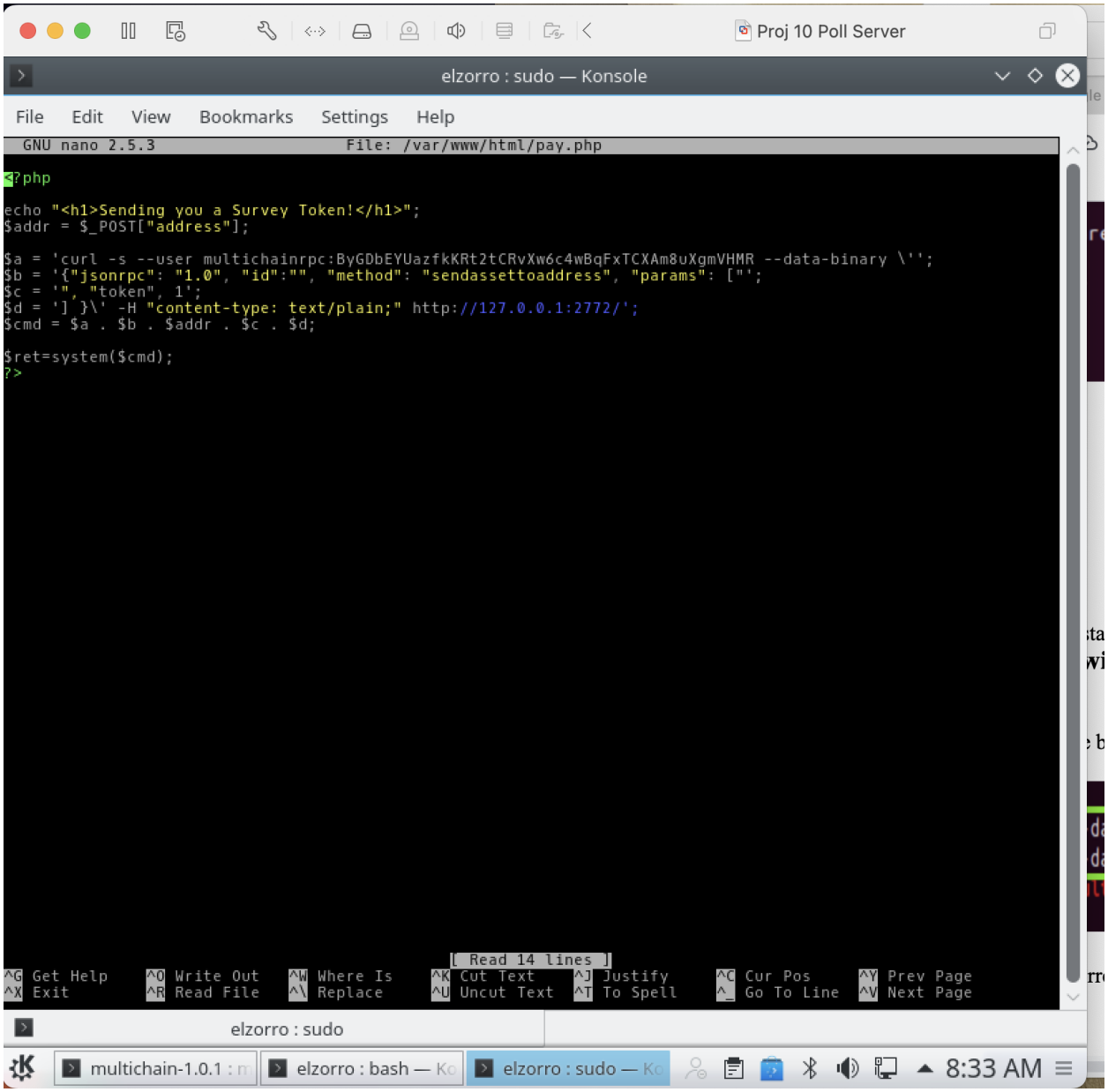
Go to the *poll server*, run this command:

sudo nano /var/www/html/pay.php

Enter or paste in this code. You will need to change two items:

1. Replace the password in the line beginning with "$a" with the correct password on your Poll Server
2. Replace the port number at the end of the line beginning with "$d" with the actual port number on your server.

```
<?php

echo "<h1>Sending you a Survey Token!</h1>";
$addr = $_POST["address"];

$a = 'curl -s --user
multichainrpc:8EC2qNiyoyAVj6dQE6Sf5VuyVJF2zSewrsixnEMdoh7t
--data-binary \'';
$b = '{"jsonrpc": "1.0", "id":"", "method": "sendassettoaddress",
"params": ["';
$c = '", "token", 1';
$d = '] }\' -H "content-type: text/plain;" http://127.0.0.1:9706/';
$cmd = $a . $b . $addr . $c . $d;

$ret=system($cmd);
?>
```



16) Make a faucet.htm Page

Go to the *poll server*, run this command:

sudo nano /var/www/html/faucet.htm

Enter or paste in this code.

<html><head><title>Survey Token Faucet</title></head>
<body bgcolor="#cccccc">
<h1 align="center">Survey Token Faucet</h1>

```
<form method="post" action="pay.php">
<p align="center"><b>Enter your address</b></p>
<p align="center"><input type="text" name="address"
size="90"></textarea></p>
<p align="center">
<button type="submit" name="submitButton" value="">Get Token</button>
</form>

</body></html>
```

17) Removing Old Multichains on the Voter

Go to the *voter server*, run this command:

ps aux | grep multi

As a result if any Multichain daemon is running you will see on the right hand side with the command line argument. Note down the id number for the next step.

For each and every multichain process execute this command to kill it:

kill 19066(change process as per yours)

Execute this command to remove the old multichain data form the server:

rm -rf ~/. multichain

18) Install Multichain on the Voter

Go to the *voter server*, run this command:

cd /tmp

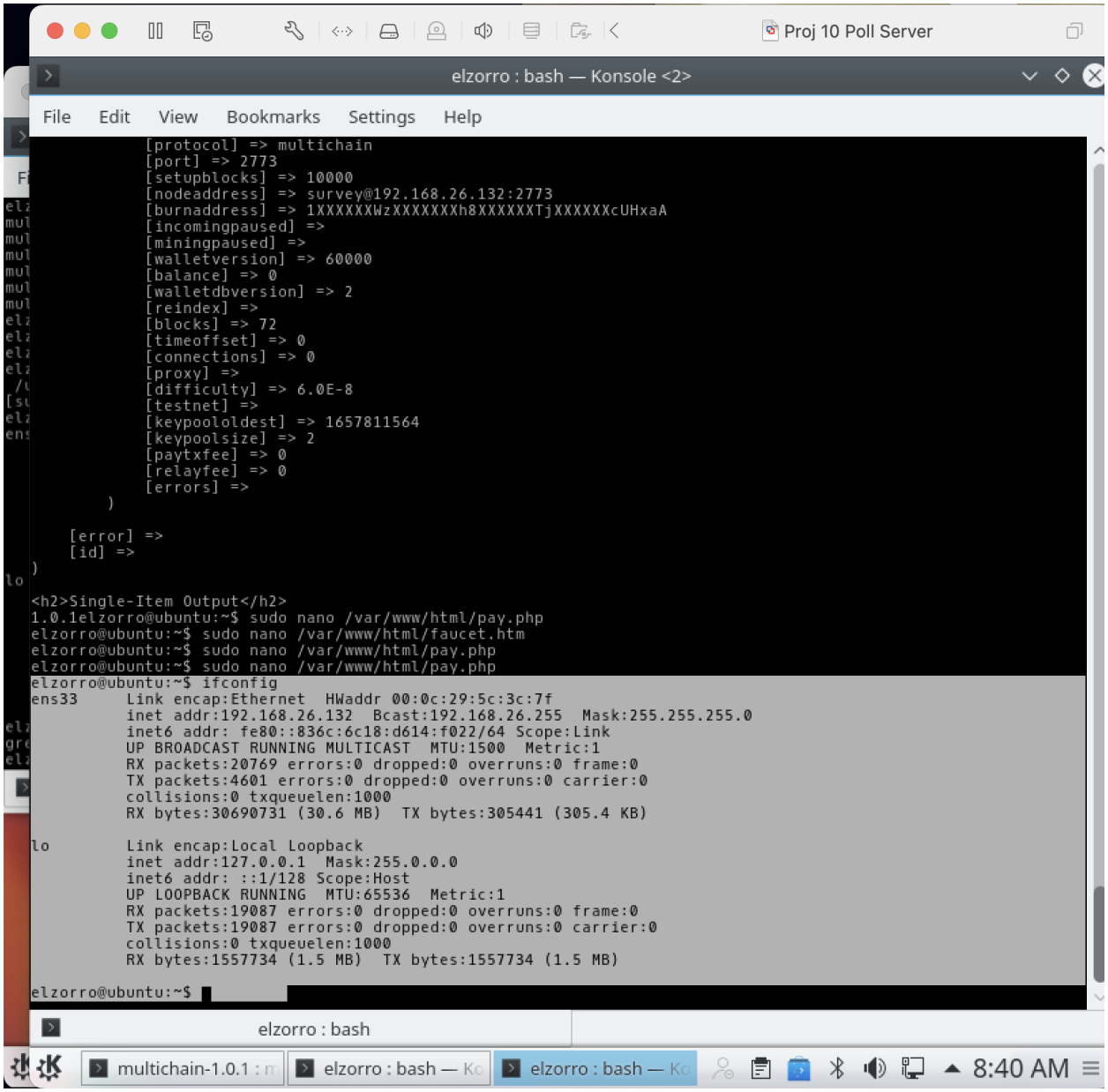
wget http://www.multichain.com/download/multichain-1.0.1.tar.gz
tar -xvzf multichain-1.0.1.tar.gz
cd multichain-1.0.1
sudo mv multichaind multichain-cli multichain-util /usr/local/bin

19) Finding the IP Address of your Poll Server

Go to the *poll server*, run this command:

ifconfig

As shown below, find the IP address of your Ethernet interface.



20) Finding the Network Port

Go to the *poll server*, run this command:

grep network-port ~/.multichain/survey/params.dat

Find the port number, as shown below.

21) Connecting the Voter to the Blockchain

Go to the *poll server*, replacing the node address and port number with the correct values for your Poll server, which you found just one step above.

multichaind survey@172.16.1.135:9707 -daemon

22) Getting an Address

Go to the *poll server*, run this command:

multichain-cli survey getnewaddress

Make an note of address appears as result from above command.

23) Using the Faucet

Go to the *poll server or voter server*, run this command:

172.16.1.135/faucet.htm

Copy and paste your address from the Voter's page onto the Faucet page, as seen below.

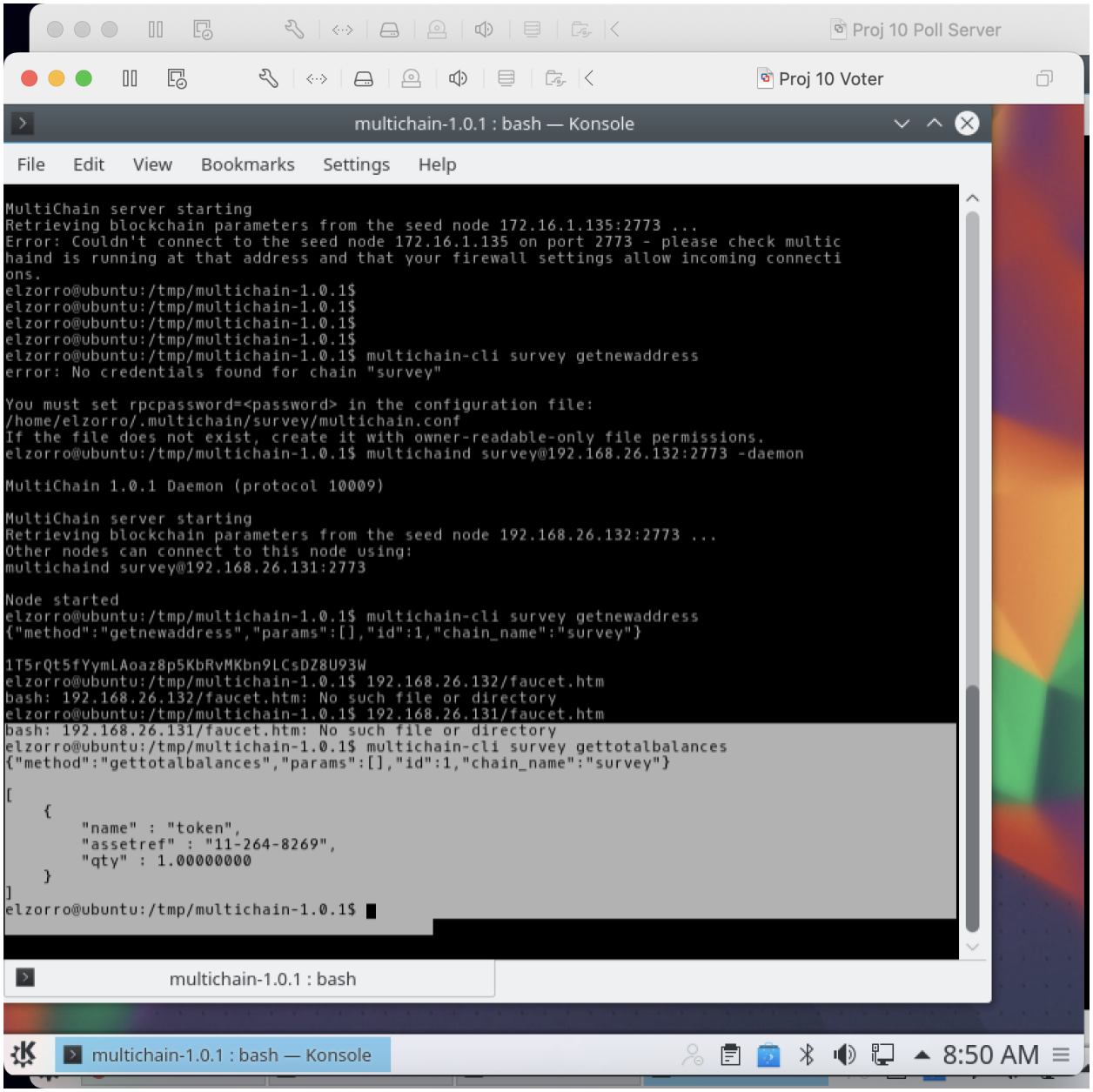
Click the "**Get Token**" button.

The response shows **"error": null**, as shown below--it worked!

24) Checking your Balance

Go to the *voter server*, run this command:

multichain-cli survey gettotalbalances

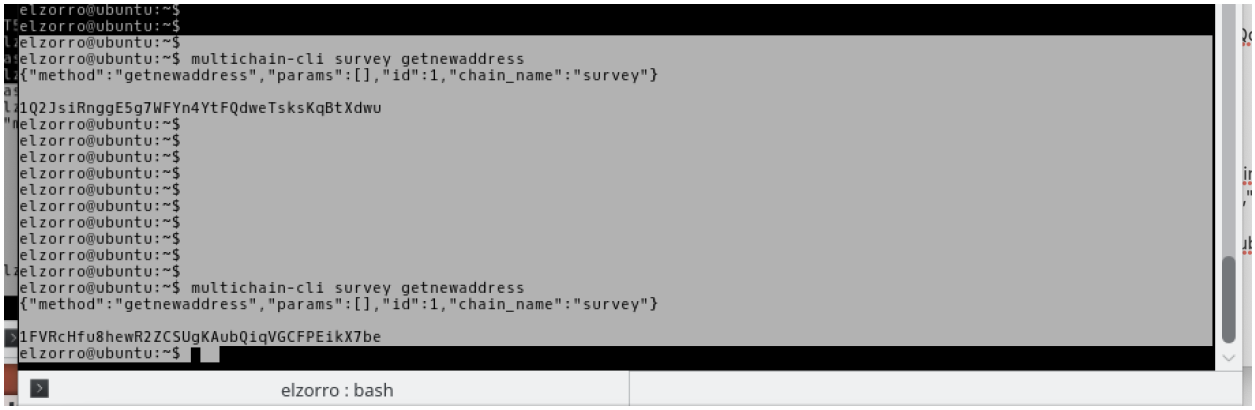


25) Getting an Account for Candidate #1

Go to the *poll server*, run this command:

multichain-cli survey getnewaddress

multichain-cli survey getnewaddress



26) Making a Voting Page

Go to the *poll server*, run this command:

sudo nano /var/www/html/vote.htm

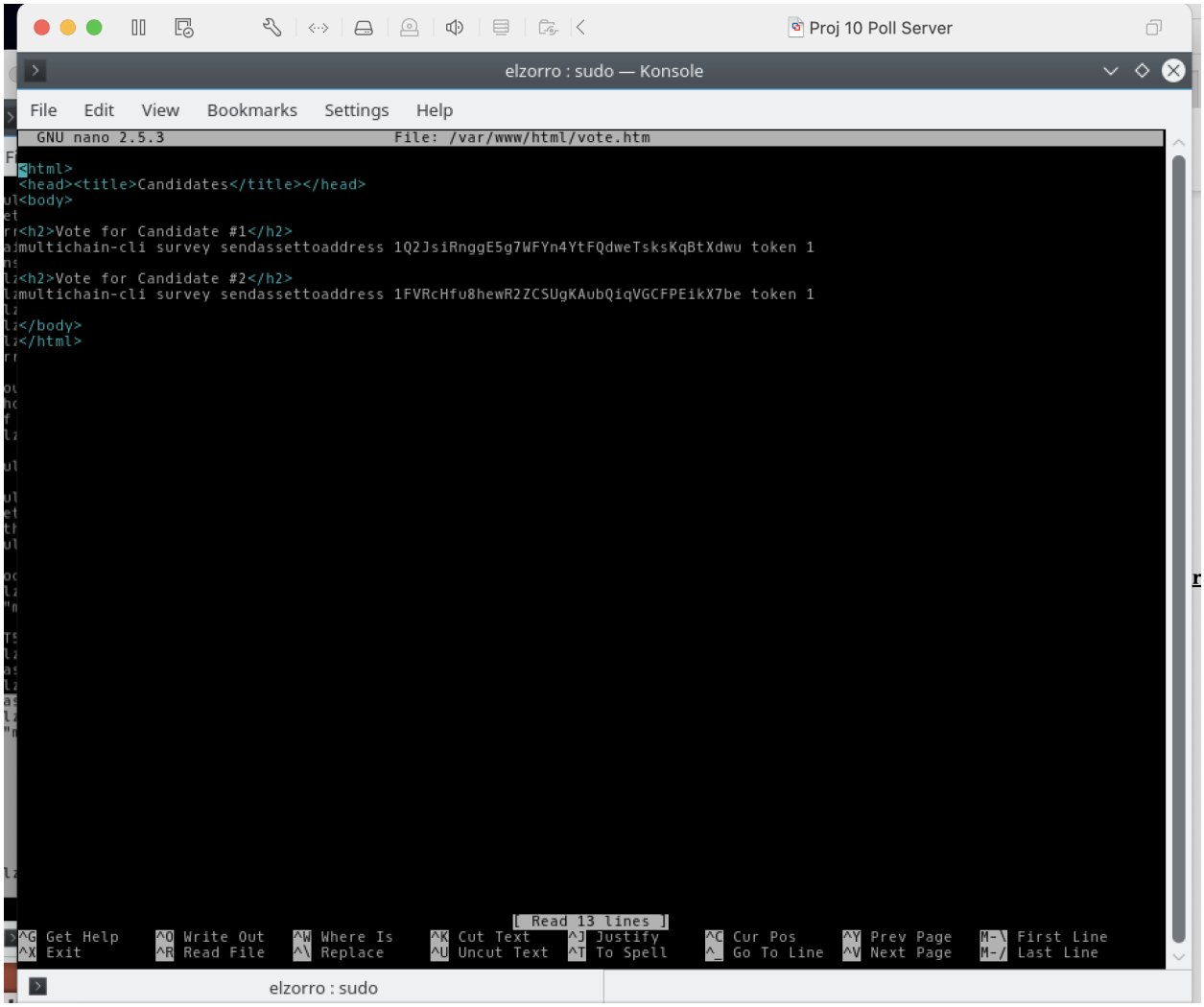
Paste in this code. Replace the addresses with the two addresses you just made.

<html>
<head><title>Candidates</title></head>
<body>

<h2>Vote for Candidate #1</h2>
multichain-cli survey sendassettoaddress 1VRxsr8G1oe9WApAXUEXT6BJ9BEjJeHJhGKTkP token 1

<h2>Vote for Candidate #2</h2>
multichain-cli survey sendassettoaddress 1M3p1VDLSfZZBERkLkERf77vZ24tf1nNhJdmYm token 1

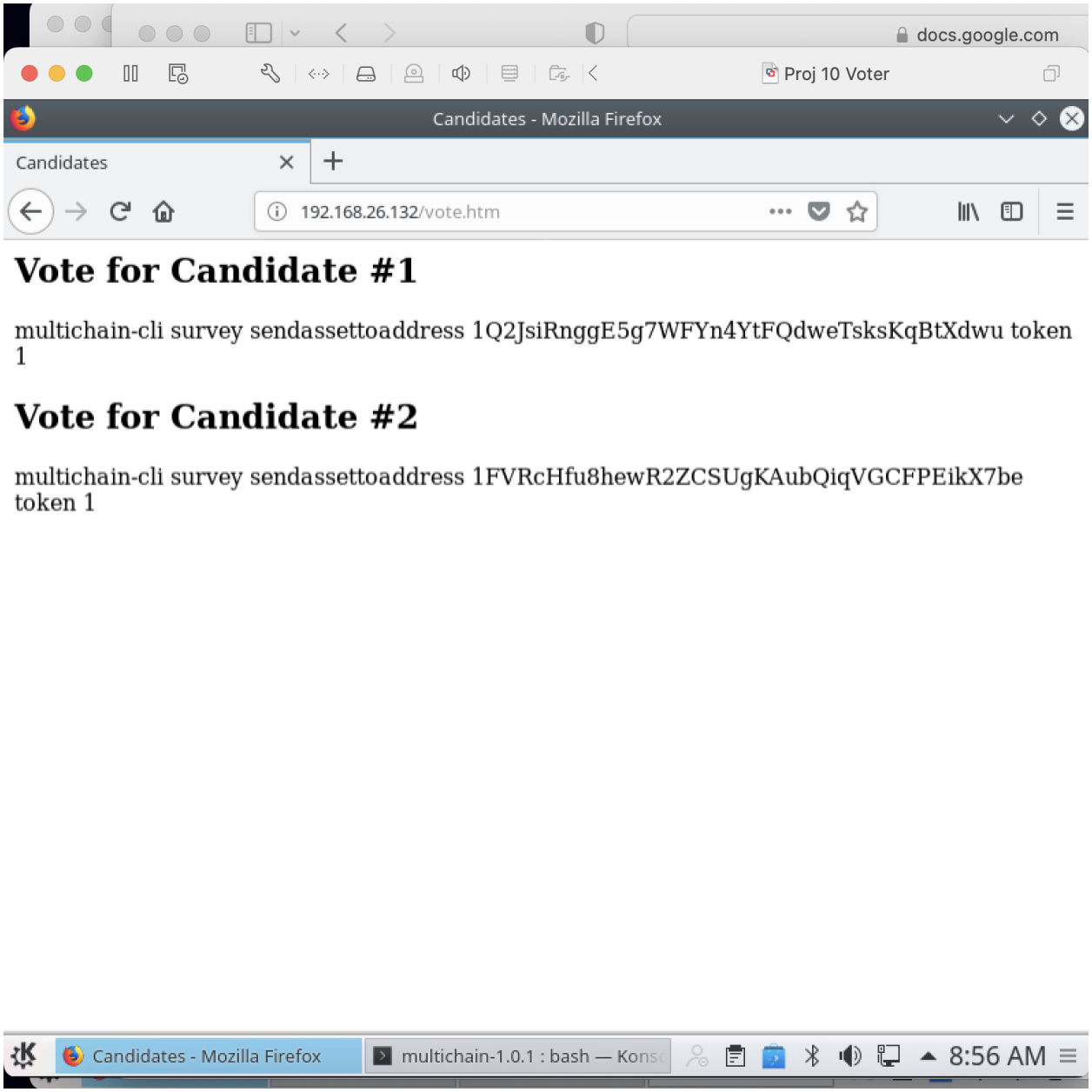
</body>
</html>



27) Voting

Go to the *Web Browser*, run this command:

172.16.1.135/vote.htm



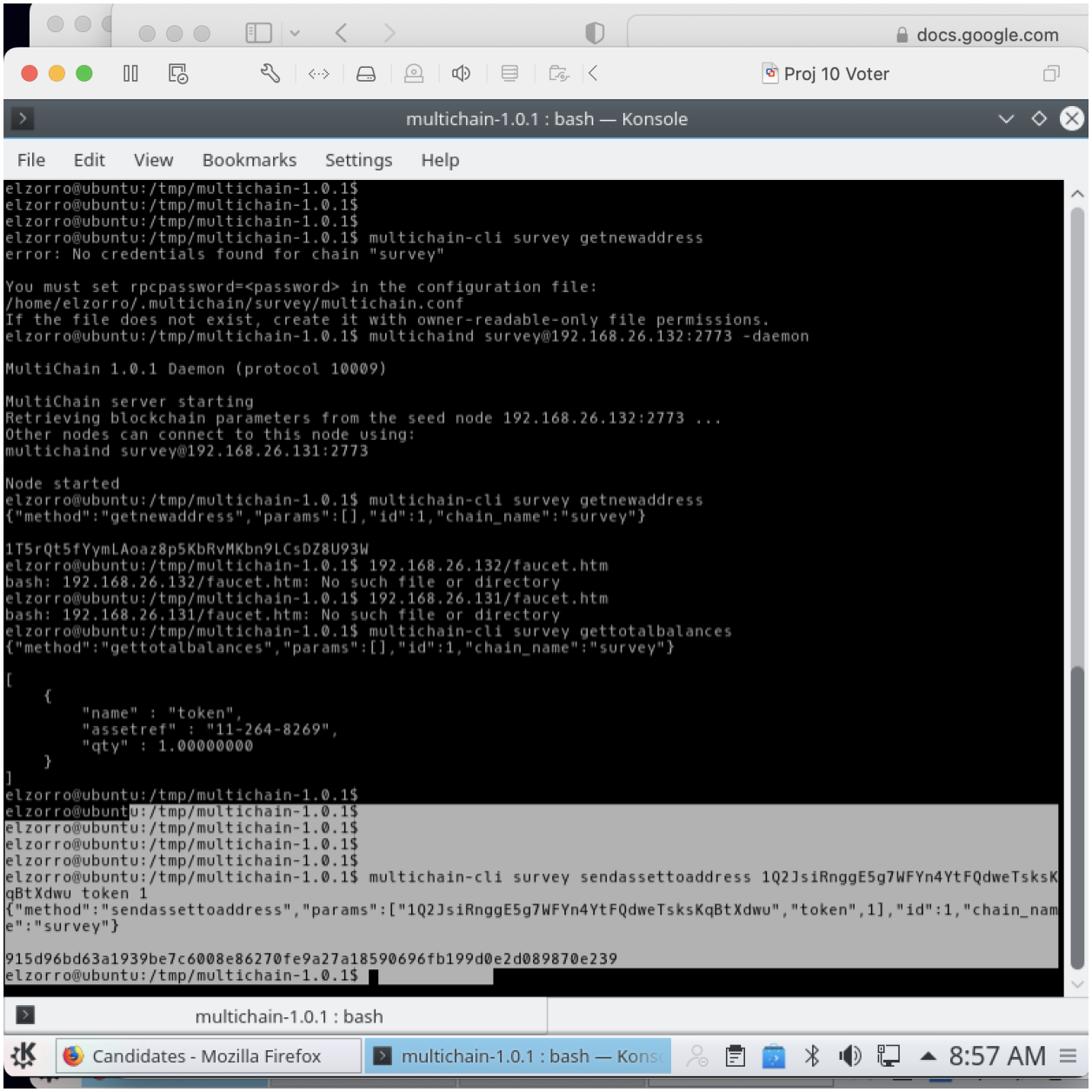
Go to the *voter server*, run this command:

Replacing the values with your candidate 1 and 2 address values, run **ONE** of the commands.

multichain-cli survey sendassettoaddress 1VRxsr8G1oe9WApAXUEXT6BJ9BEjJeHJhGKTkP token 1

OR

multichain-cli survey sendassettoaddress 1M3p1VDLSfZZBERkLkERf77vZ24tf1nNhJdmYm token 1



28) Make the results.php Script

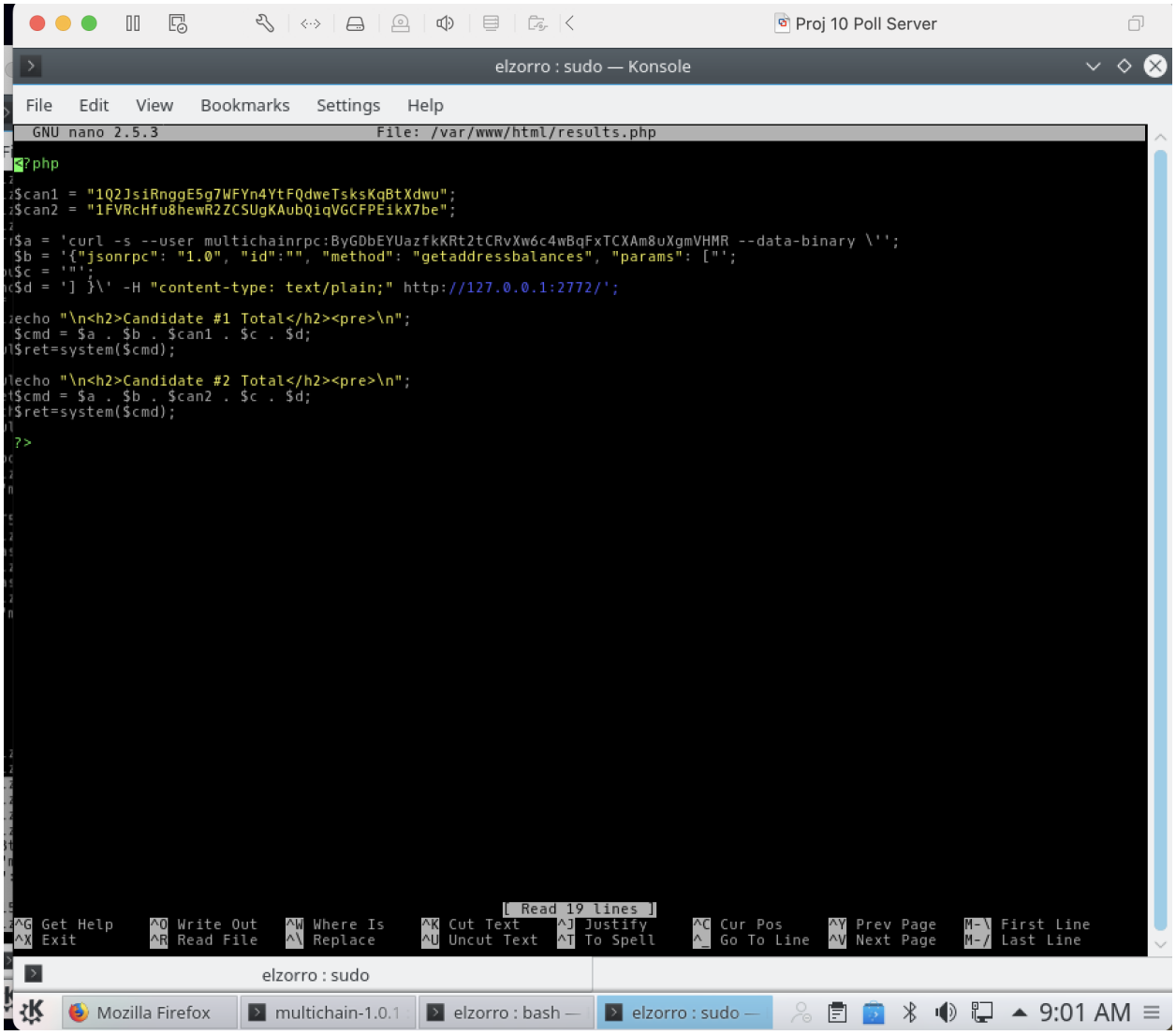
Go to the *poll server*, run this command:

sudo nano /var/www/html/results.php

Enter or paste in this code. You will need to change four items:

1. Replace the $can1 value with the address for Candidate #1
2. Replace the $can2 value with the address for Candidate #2
3. Replace the password in the line beginning with "$a" with the correct password on your Poll Server
4. Replace the port number at the end of the line beginning with "$d" with the actual port number on your server.

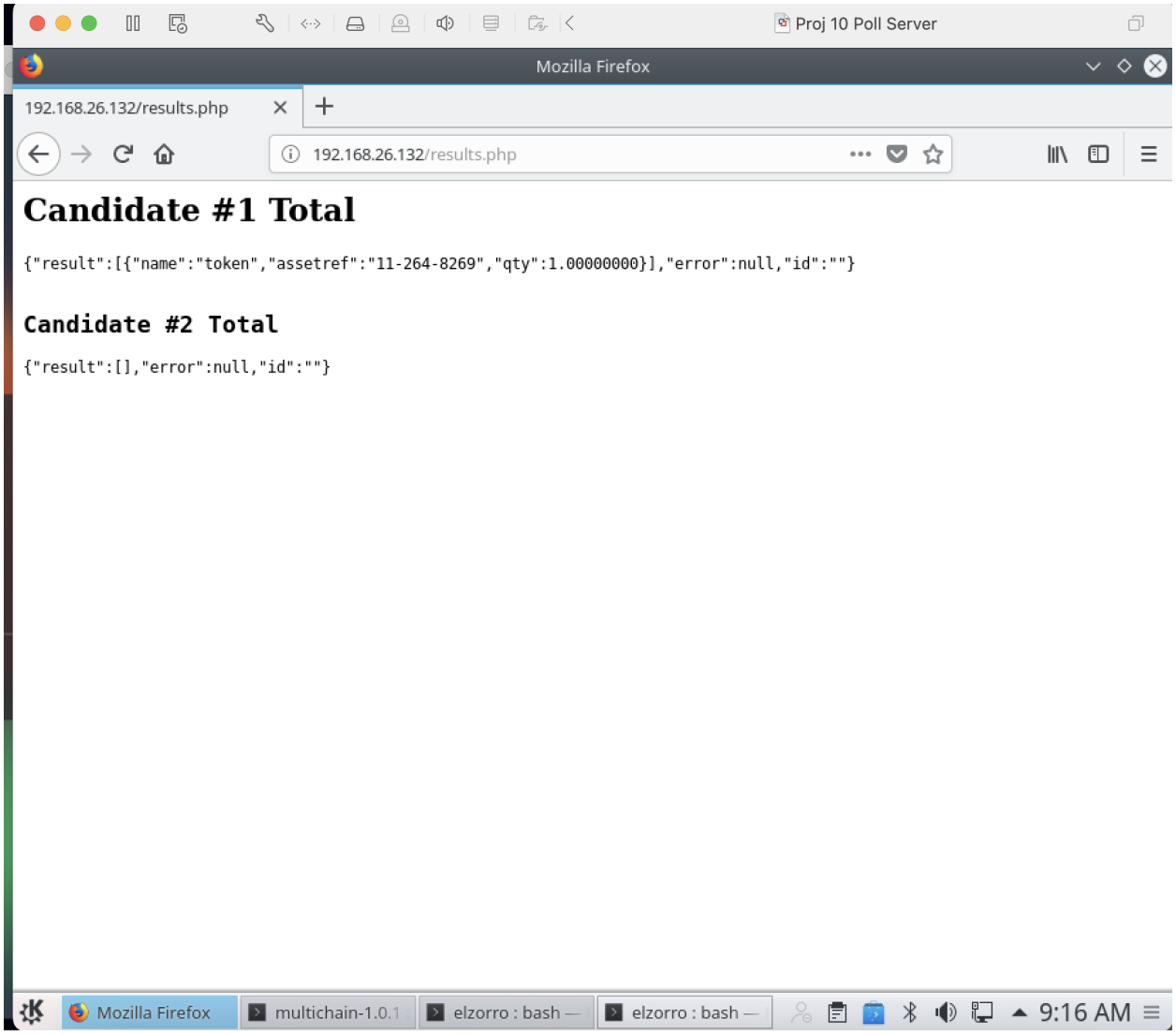
```
<?php


$can1 = "1VRxsr8G1oe9WApAXUEXT6BJ9BEjJeHJhGKTkP";
$can2 = "1M3p1VDLSfZZBERkLkERf77vZ24tf1nNhJdmYm";

$a = 'curl -s --user
multichainrpc:8EC2qNiyoyAVj6dQE6Sf5VuyVJF2zSewrsixnEMdoh7t
--data-binary \'';
$b = '{"jsonrpc": "1.0", "id":"", "method": "getaddressbalances",
"params": ["';
$c = '"';
$d = '] }\' -H "content-type: text/plain;" http://127.0.0.1:9706/';

echo "\n<h2>Candidate #1 Total</h2><pre>\n";
$cmd = $a . $b . $can1 . $c . $d;
$ret=system($cmd);

echo "\n<h2>Candidate #2 Total</h2><pre>\n";
$cmd = $a . $b . $can2 . $c . $d;
$ret=system($cmd);

?>
```



29) Viewing the Results

Go to the *Web Browser*, run this command:

172.16.1.135/results.php



30) Save Screenshot of image showing qty.

CONCLUSION : Finally, we demonstrated how to design a voter system that is secure and allows the user to confirm that his vote was accurately delivered. We did this with the help of multichain and php code for producing tokens, which were supposed to be limited to one per user but did not work, allowing users to gain several tokens and vote multiple times.