**Team based Project – Round Three Submission**

**Project Title**: Accessing Windows 11 while enabling Windows defender and firewall

**Team Members:**

1. Venkat Nithin Atturu – vatturu@ttu.edu - R11796416
2. Sulakshana Mucheli – smucheli@ttu.edu - R11842834
3. Nagavarshini Surapaneni – nasurapa@ttu.edu - R11845738

**Goal:** Accessing Windows 10 and 11 operating system and manipulating the file system of OS

**Programming language used:** Python

**Abstract:**

In this project, we access the system-level information on the victim's computer using python code. Once the code gets executed on the victim's computer, we will have all the access to the computer, and we can inject our files to the victim's computer or copy files from the victim to the attacker's machine. We can execute all the bash commands on the victim's computer using the attacker's machine.

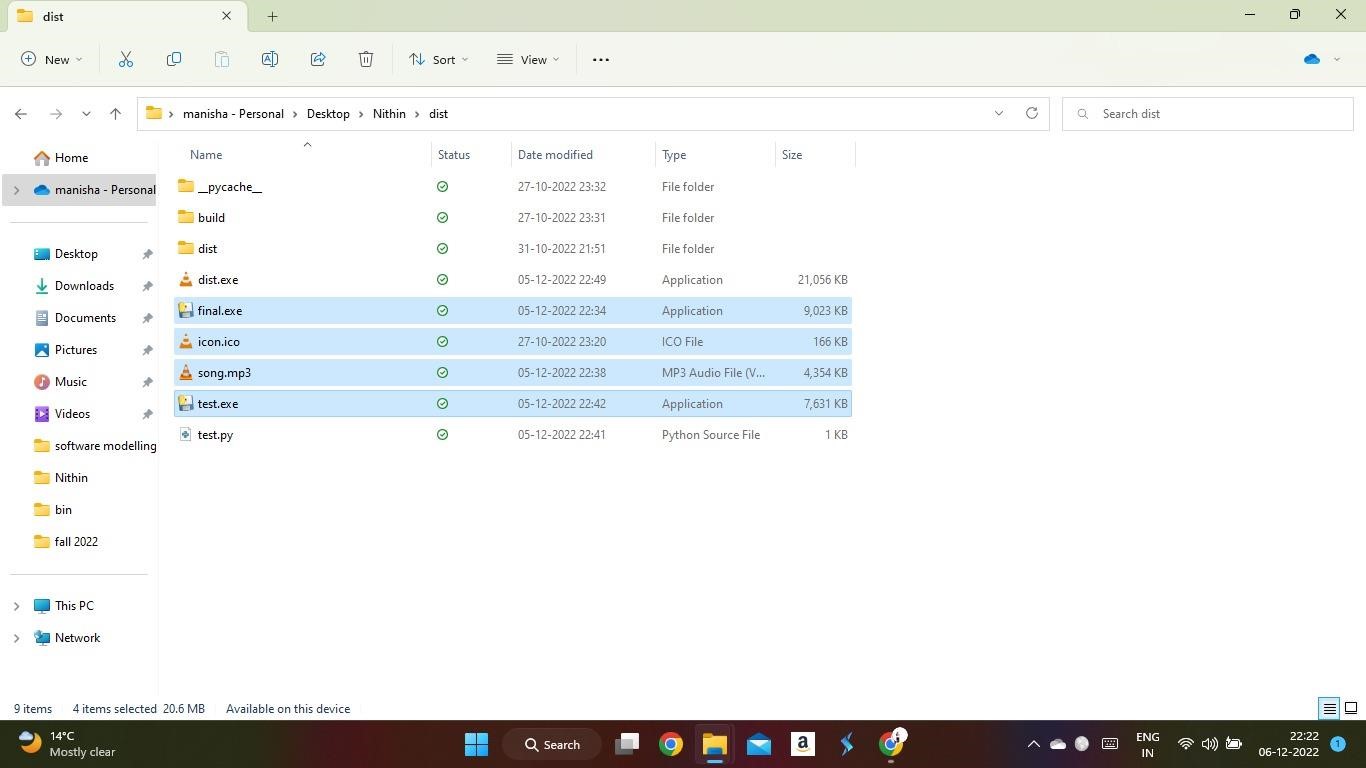
**Report of what has been done in this round**

We have embedded the python file to the Executable file, the below steps are used in making the Executable.

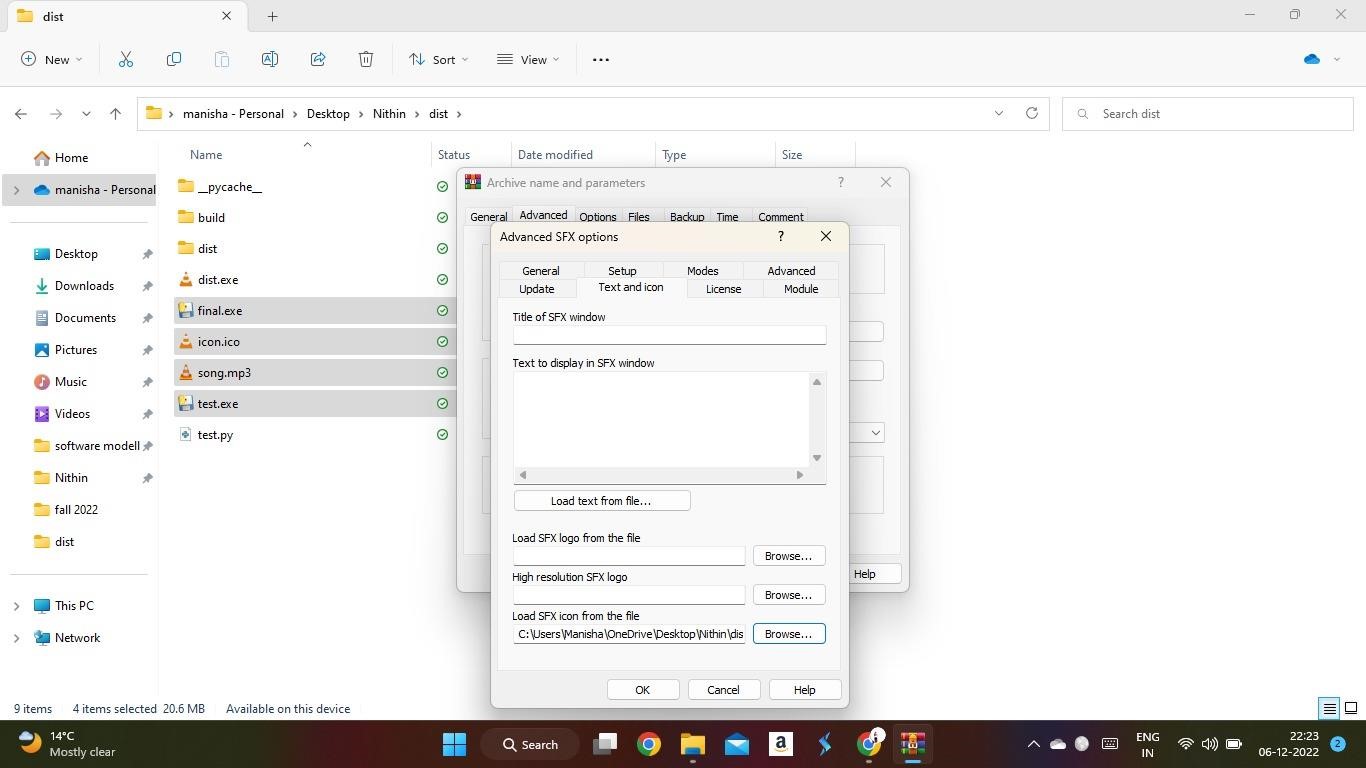
First the Python program is converted to exe, later we will use WinRAR and chose SDX options and embed the exe file to the MP3.

Here we have used WinRAR for creating the SFX archive here SFX is a computer executable program which contains compressed data in an archive file combined with machine-executables.

The below selected files are used for making the main payload.

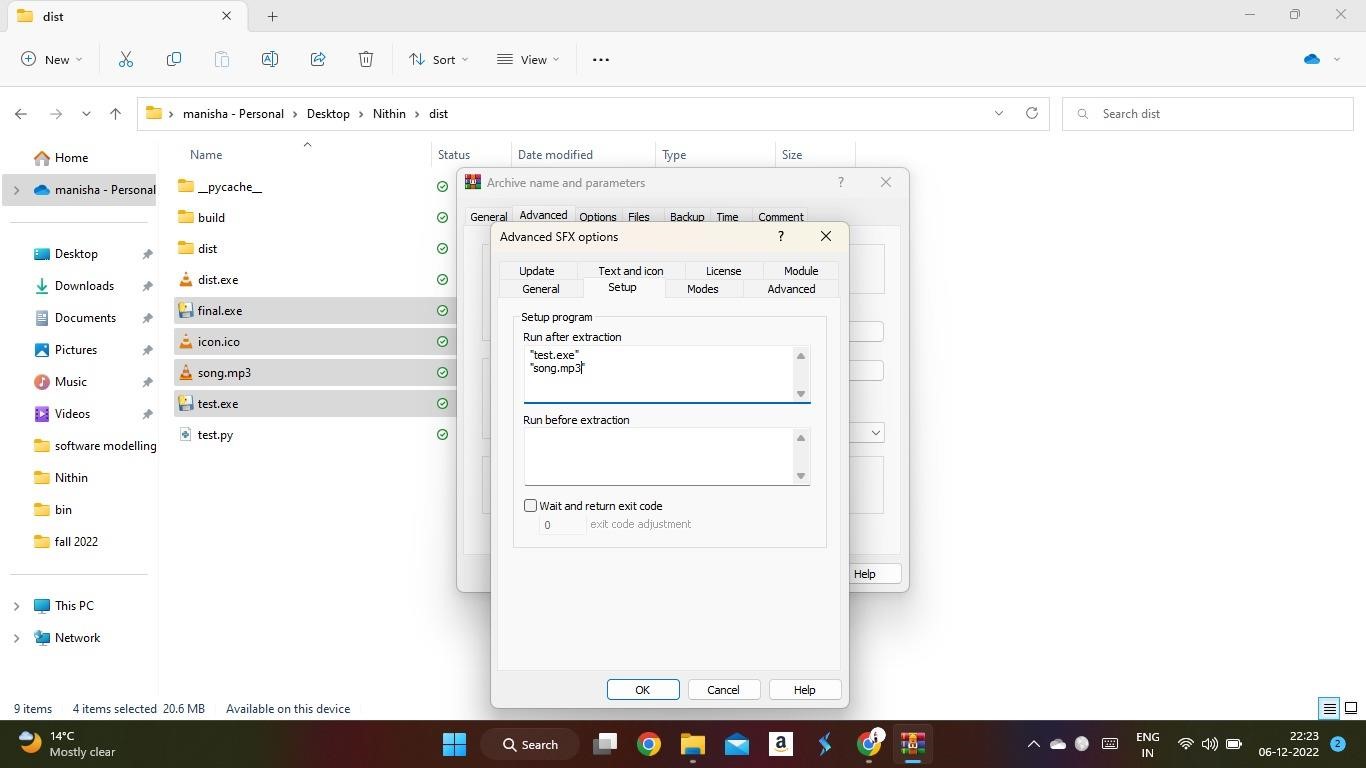


The below screen shot shows what is the path of the Icon I have selected for the Executable.



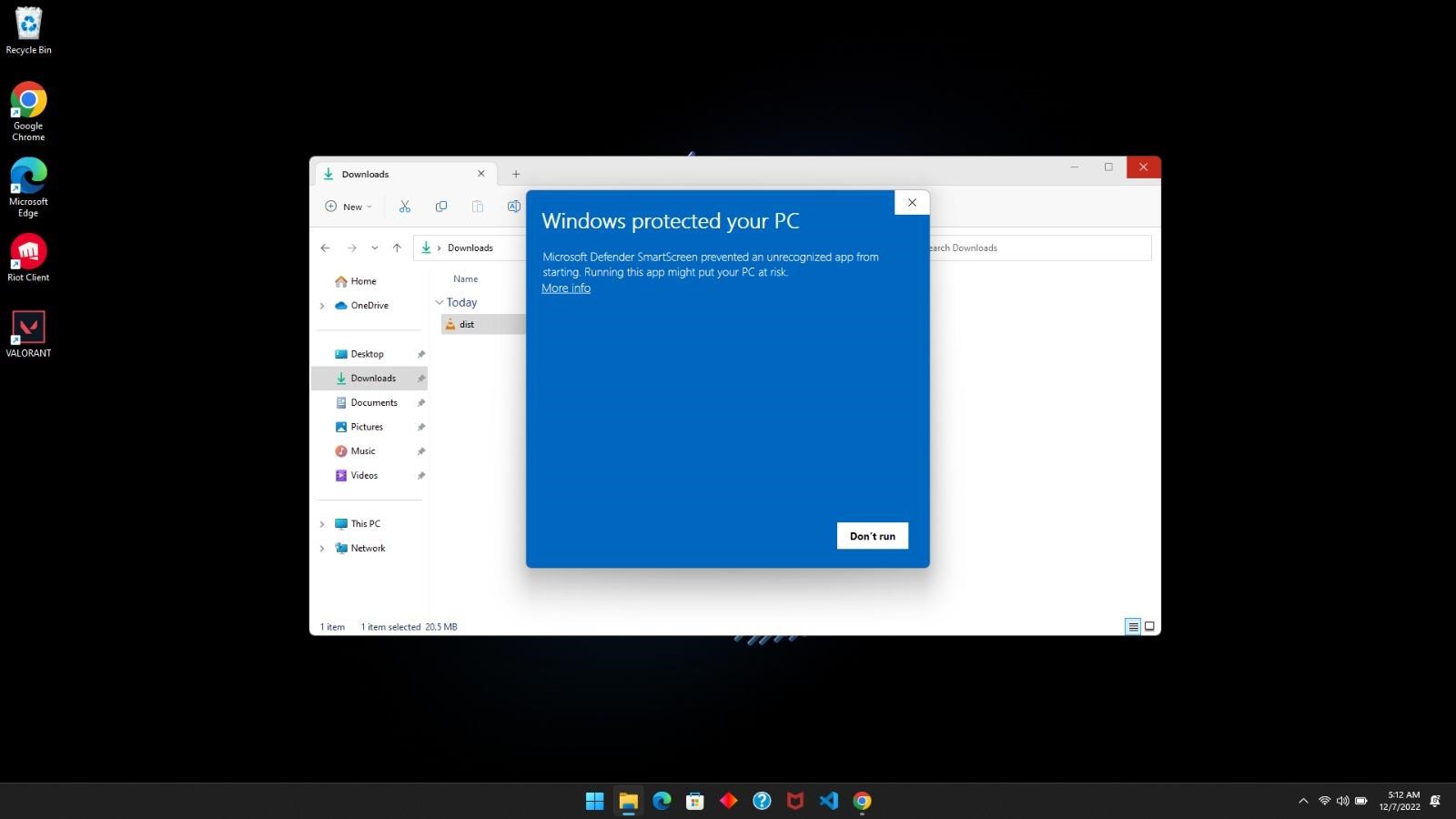
In setup tab we can instruct the exe to run what ever the program we need to execute after clicking Executable.

Here I have instructed test.exe and song.mp3 for the executable.

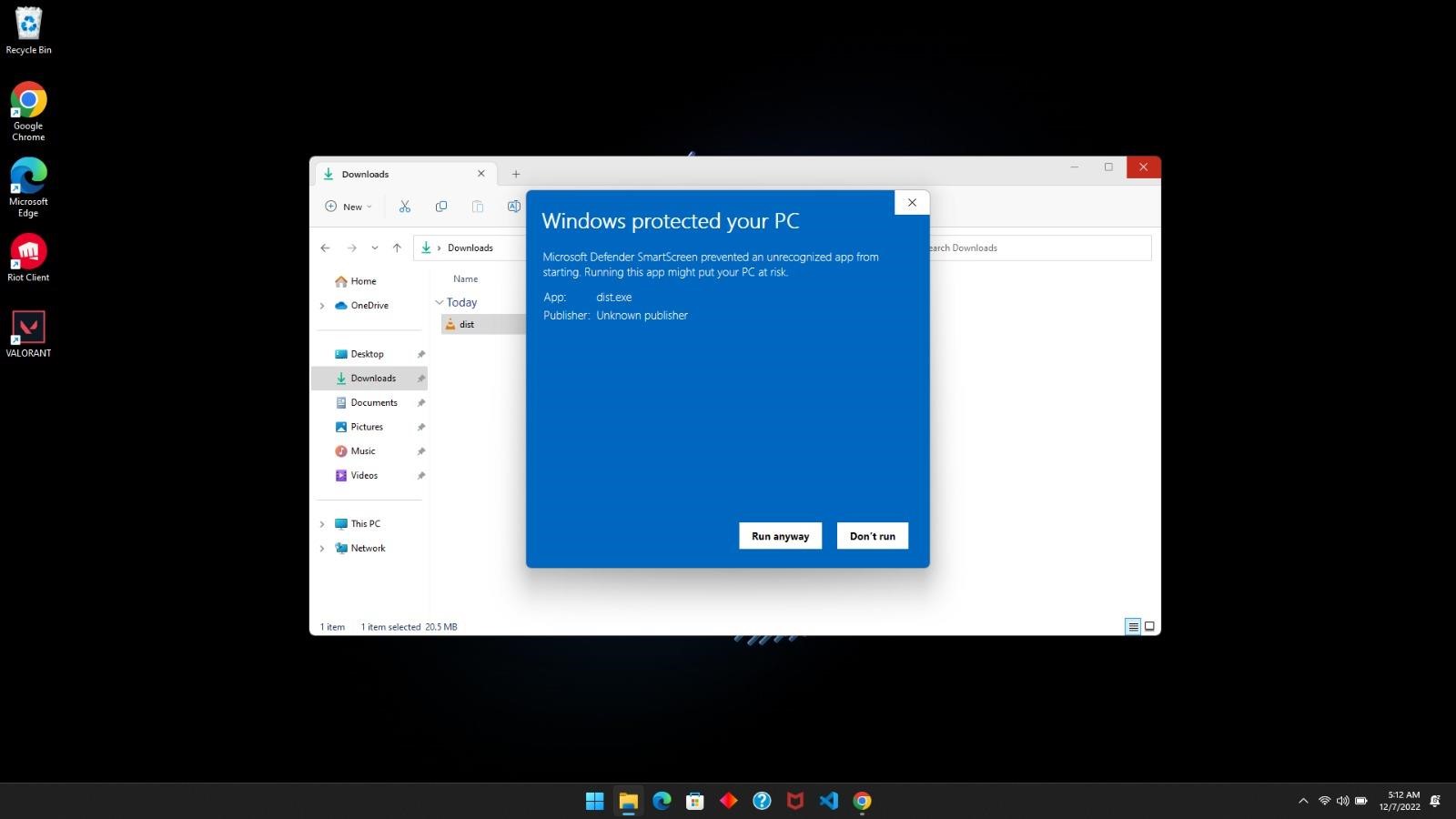


When the victim tries to open the dist.exe which is the payload file then we see a popup saying that Windows Protected your PC.

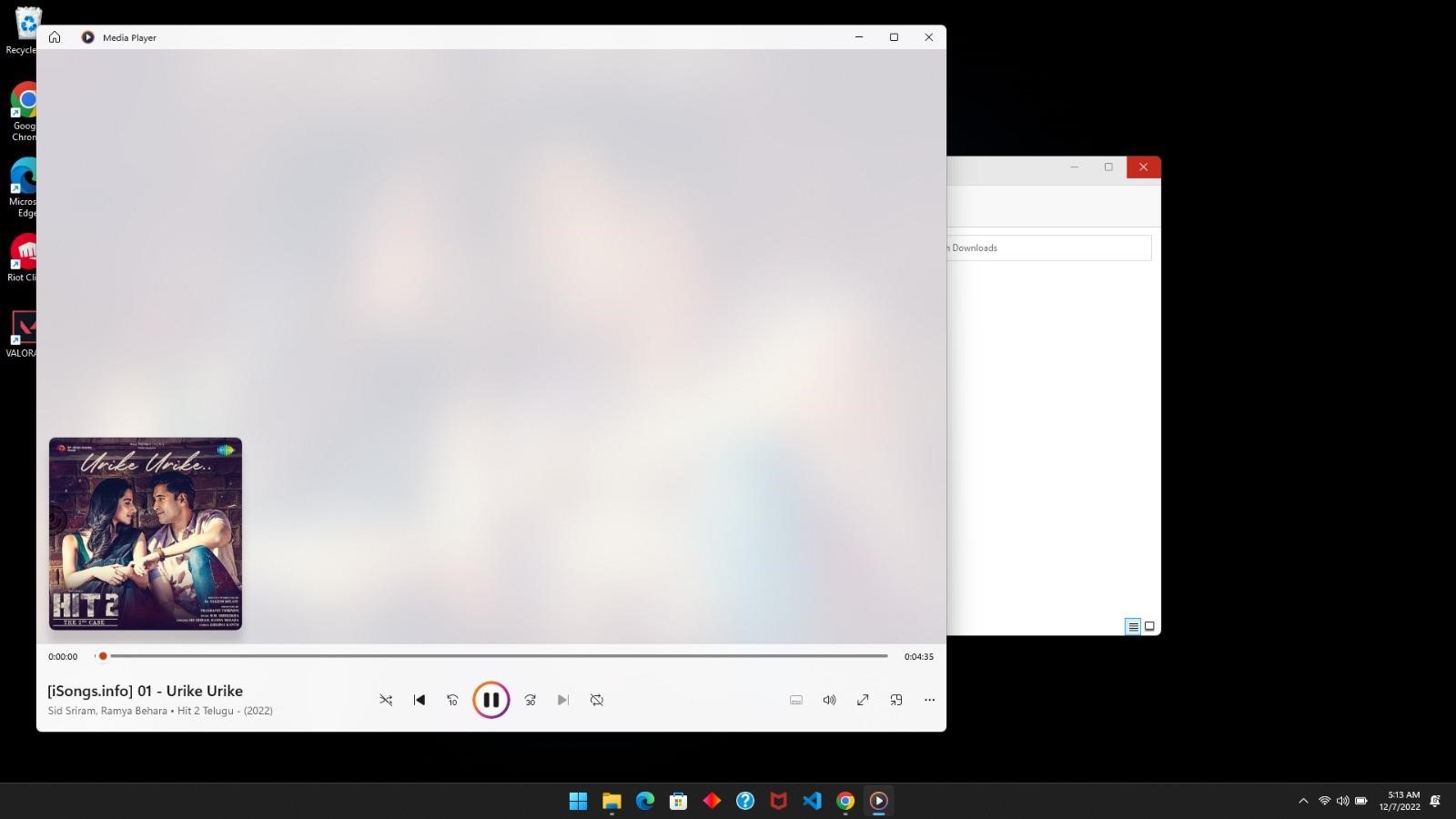
But in majority of cases when the virus file is downloaded to the computer, the file should be immediately deleted by the defender but here it is showing only the warning.



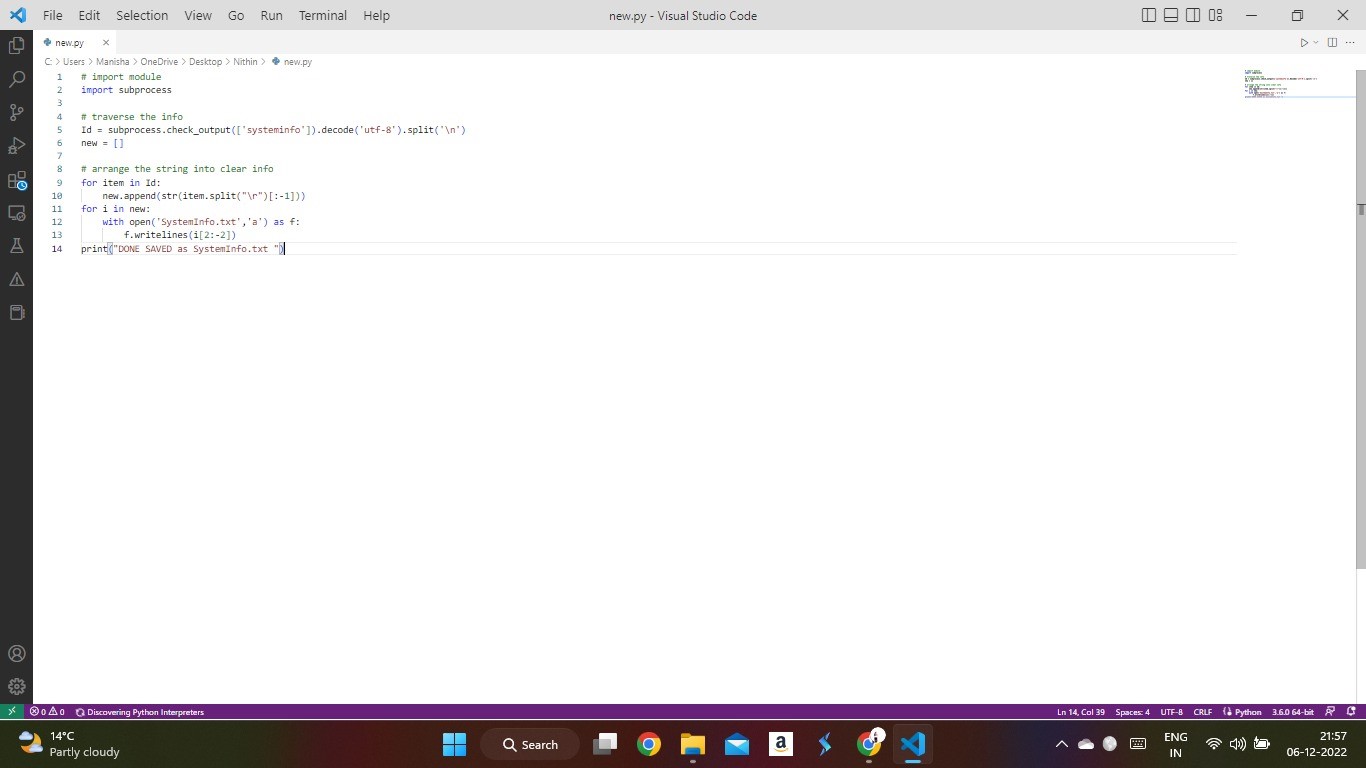
When we click on ‘More info’ we can see Run anyway button, so Defender is not considering this Executable as malware.



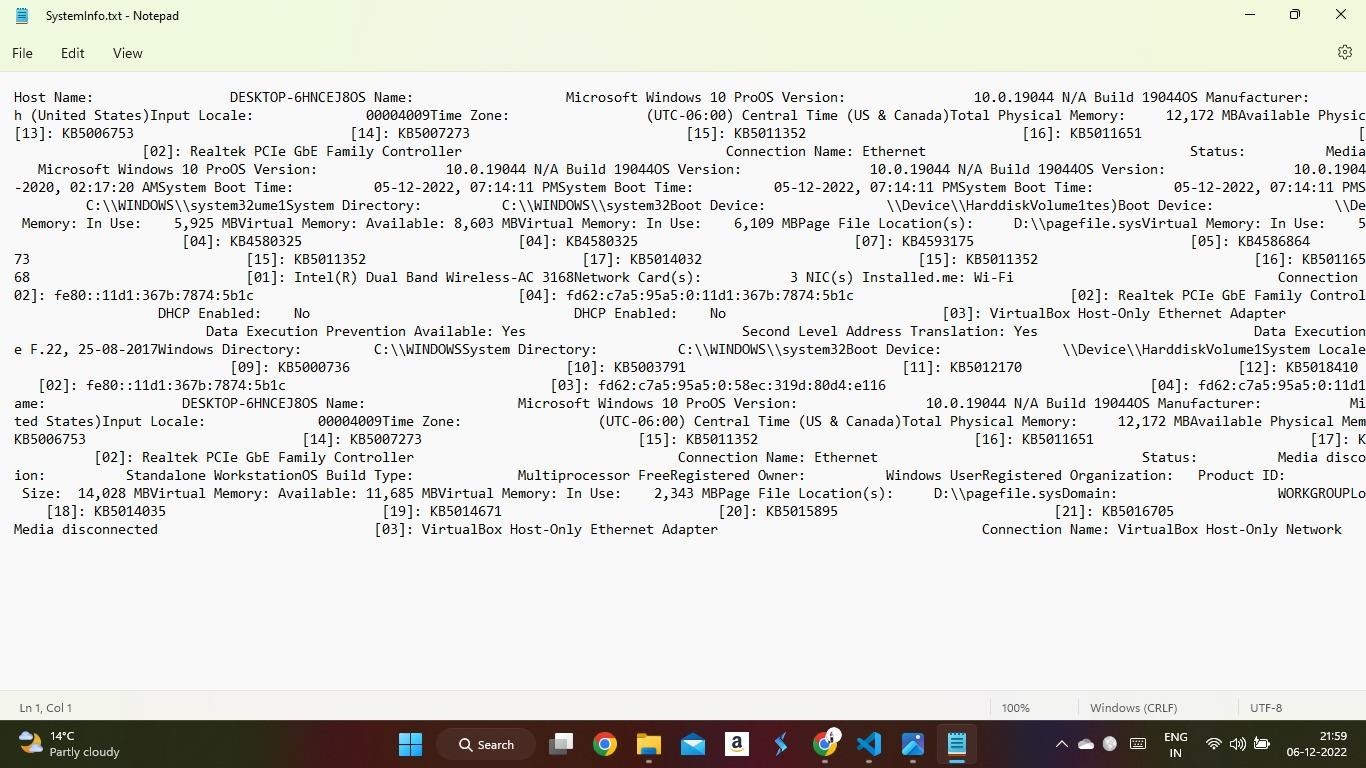
When the Victim clicks run anyway the program will get executed and will open a media player with the song playing.



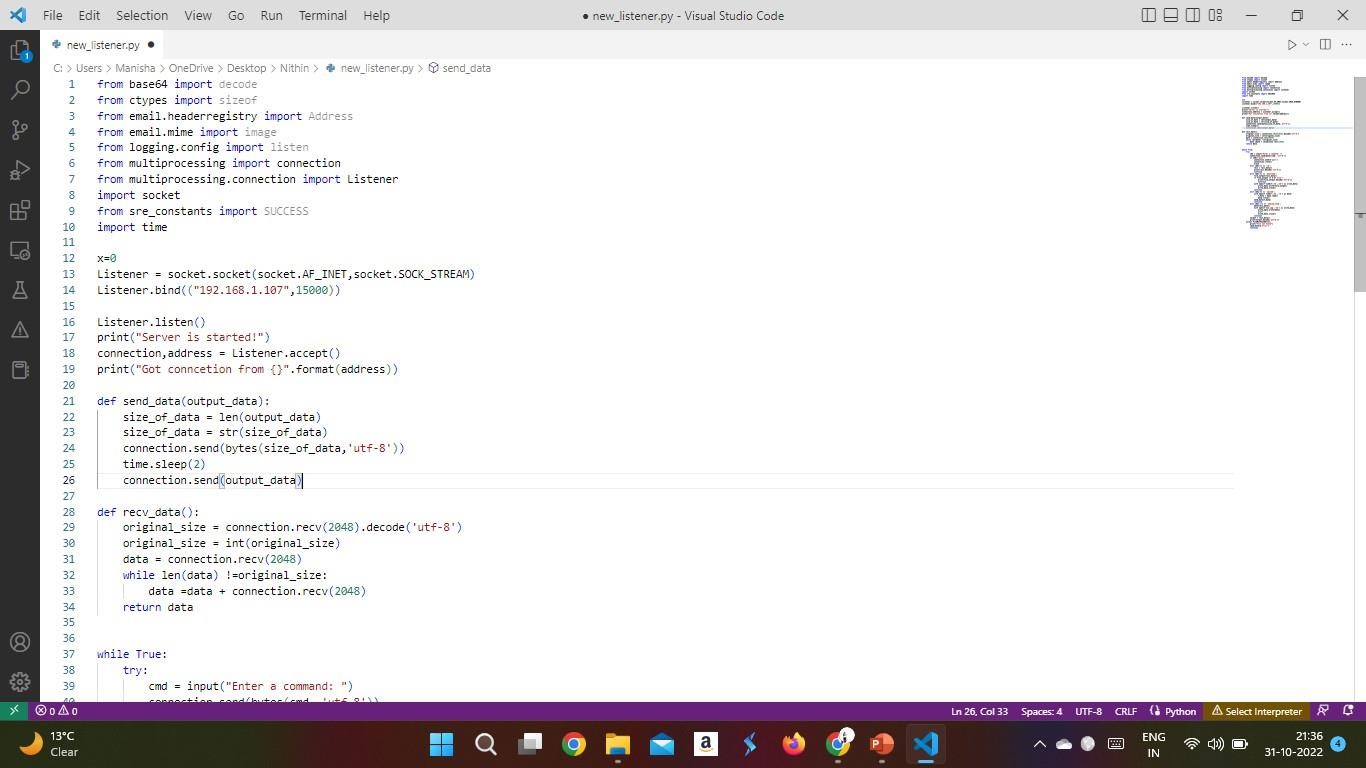
**Extracting System Level information of the victim’s computer:**

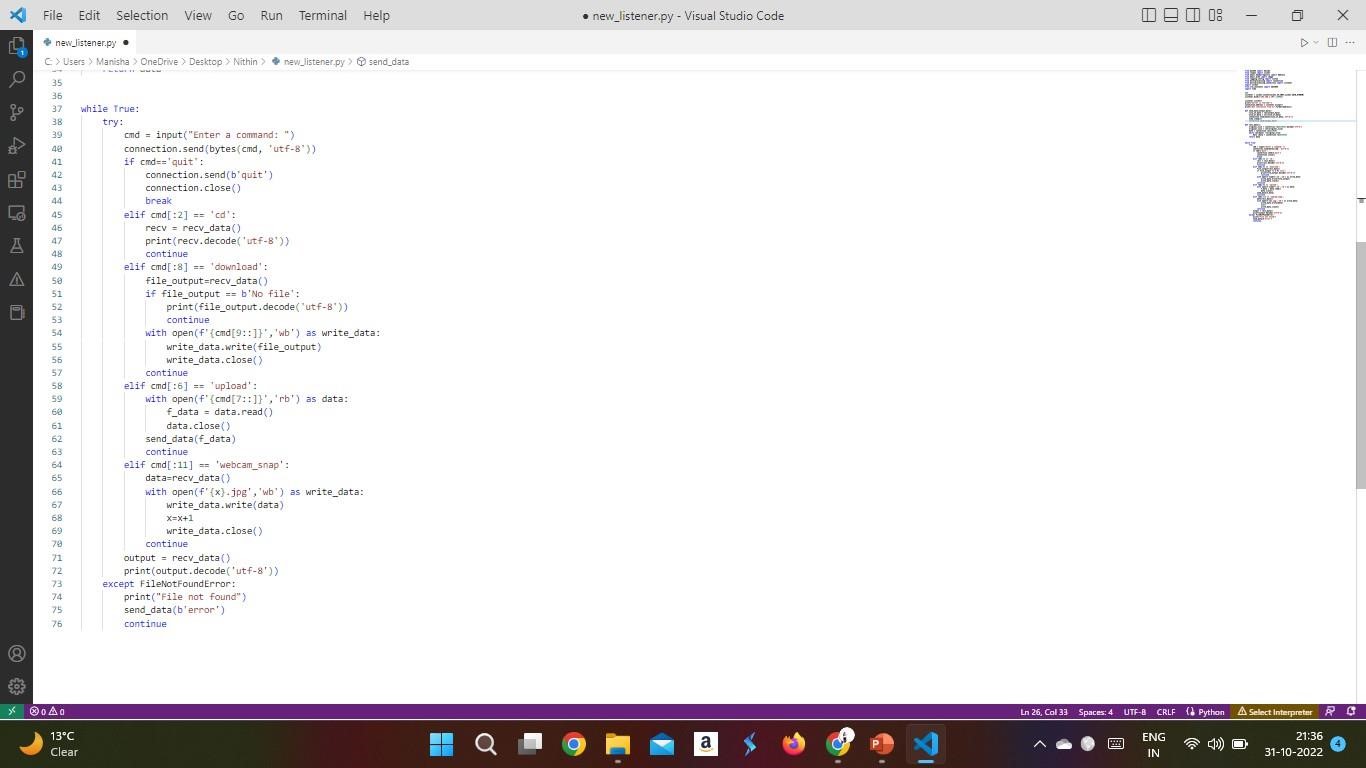


**Extracted System level information:**

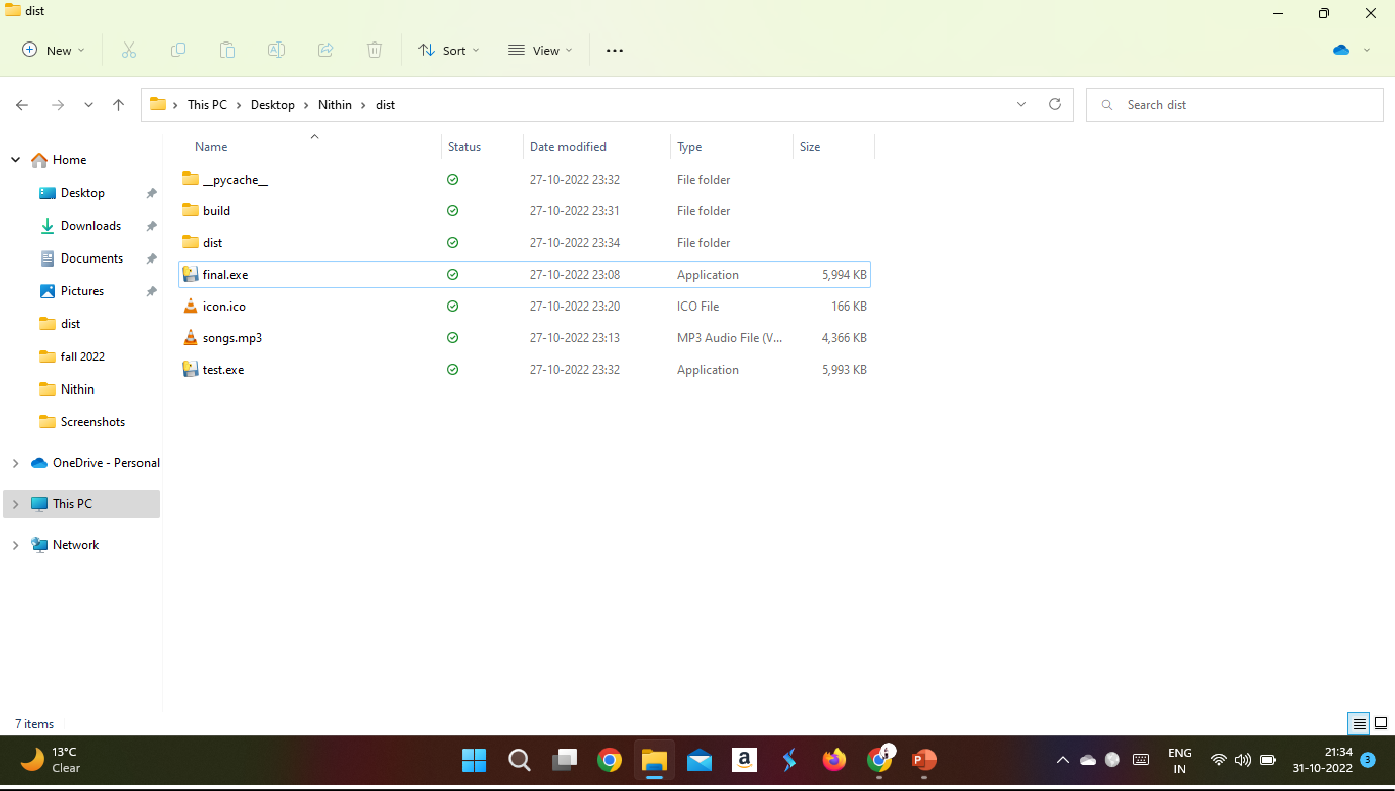


**Python code for Listener:**

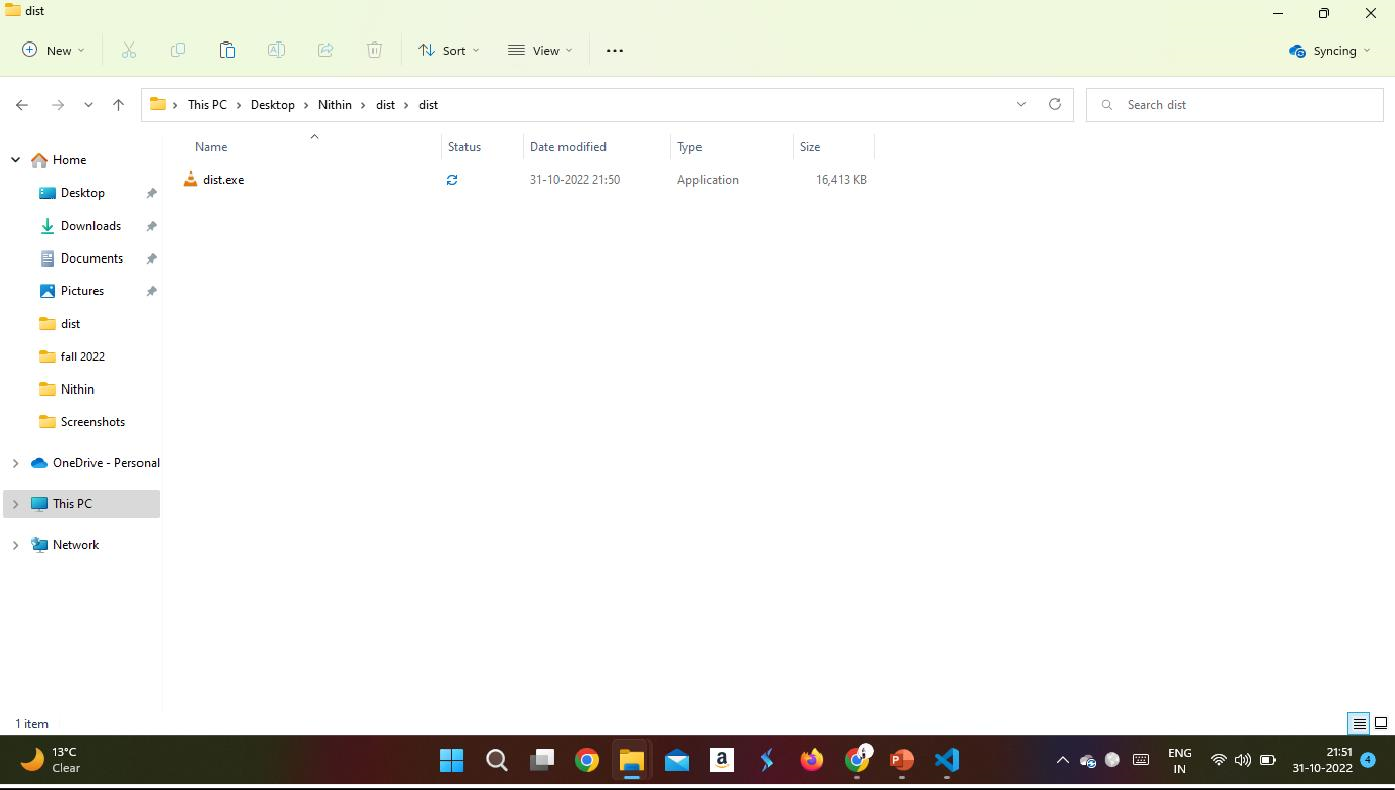




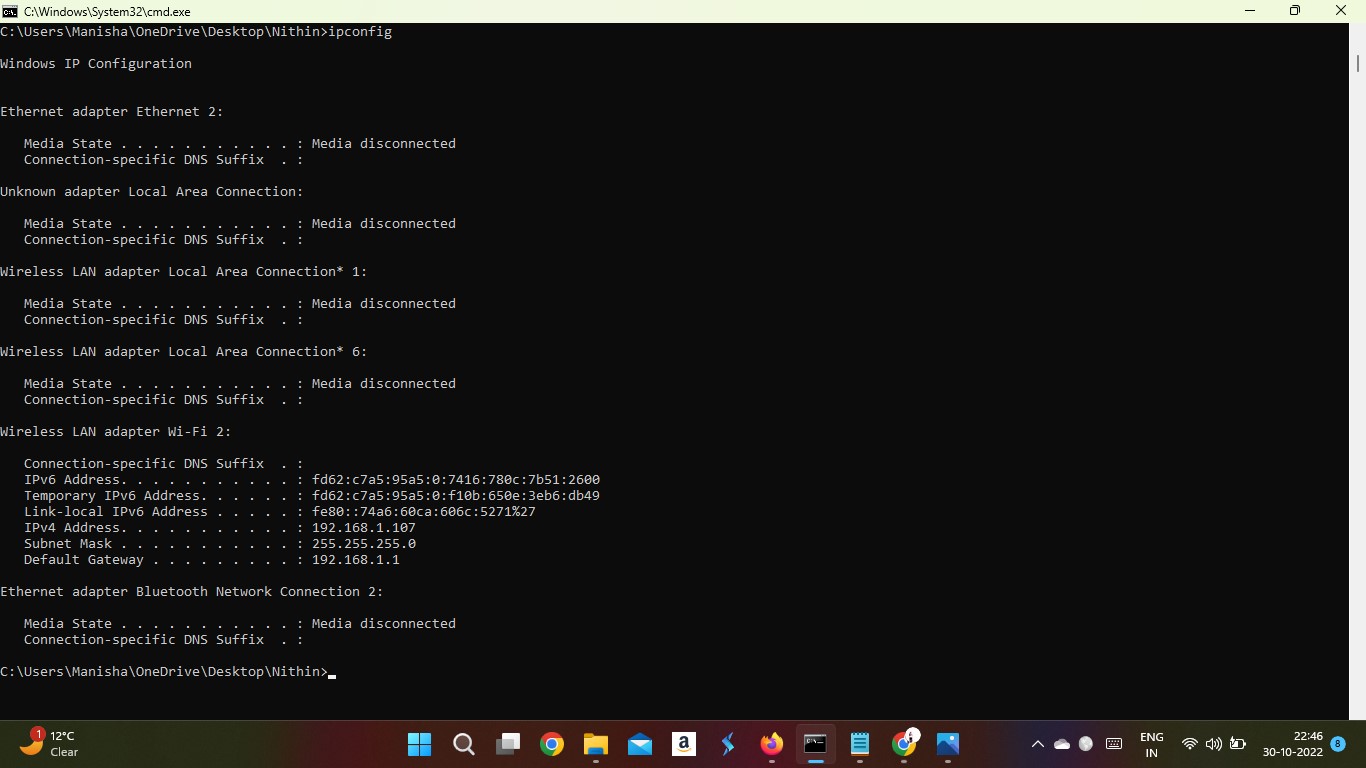
The payload file is embedded to the songs.mp3 to the final.exe which produces the dist.exe



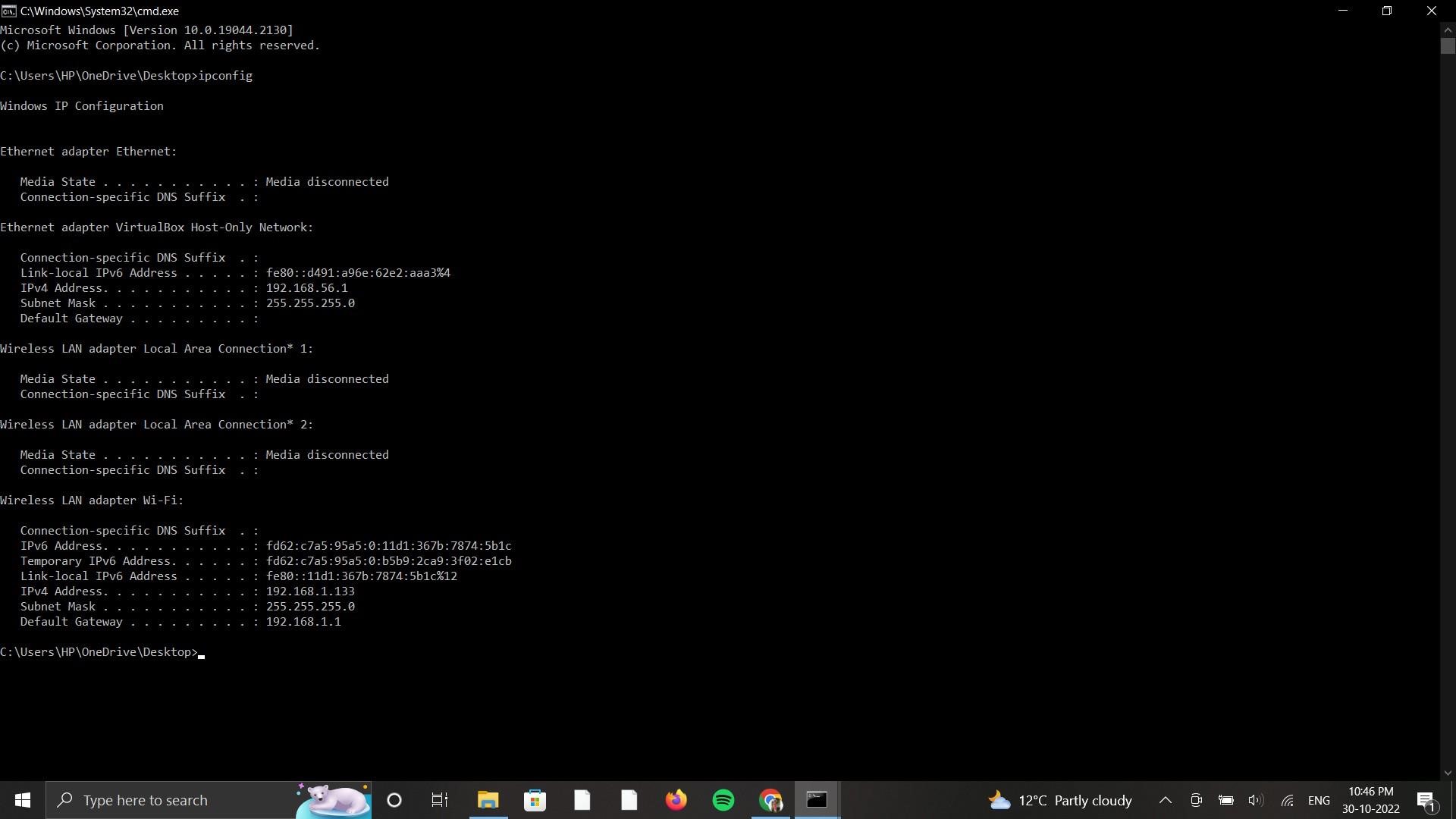
We can see that we have generated the dist.exe file, which is our main payload file, which should get executed on the victim computer.



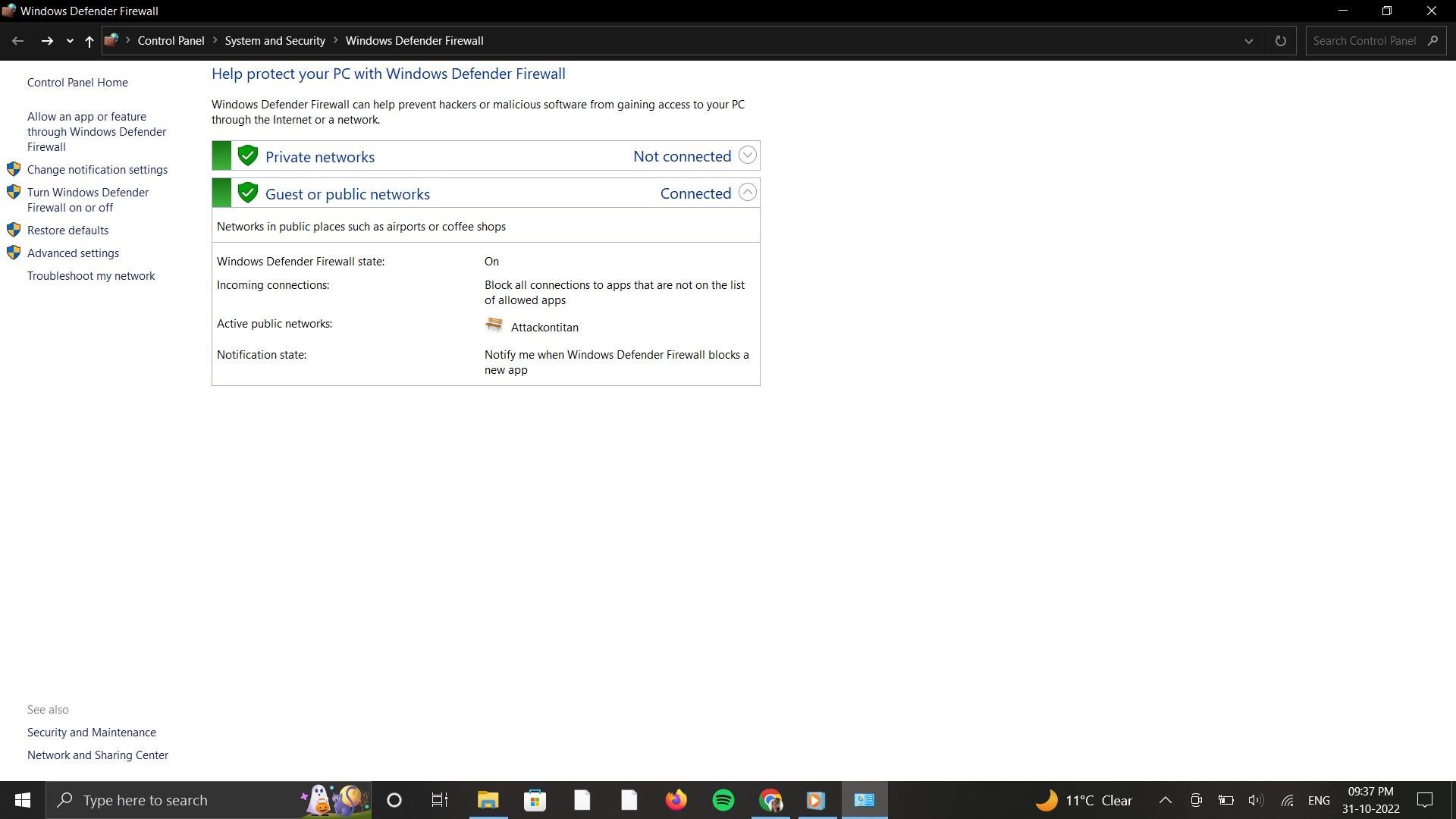
IP Address of the Attacker’s machine: 192.168.1.107



This is the IP Address of the Victim’s machine: 192.168.1.133

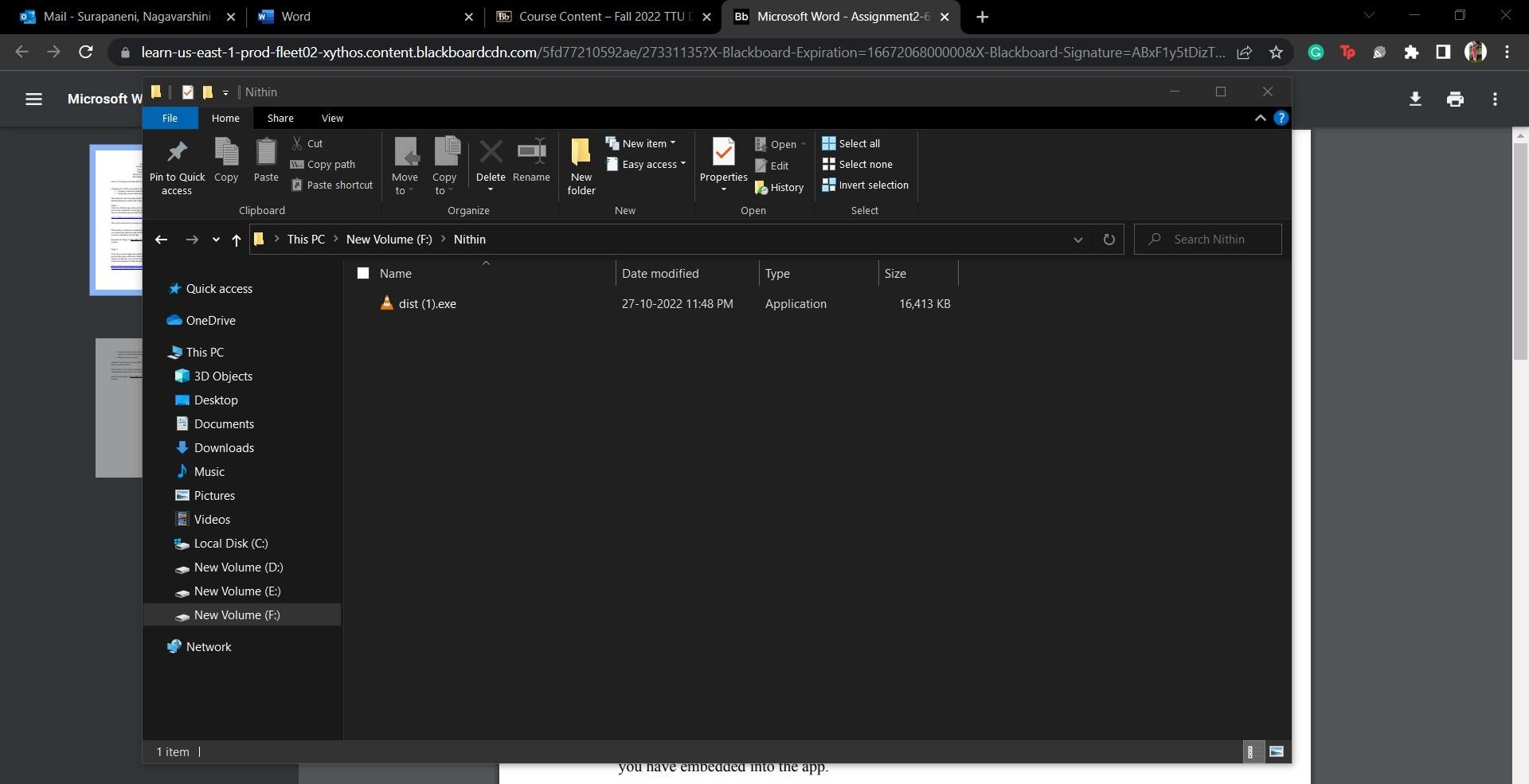


We can see that theWidows defender of the Windows 10 Operating systemis on. Though windows defender is on we can penetrate through the victim computer.

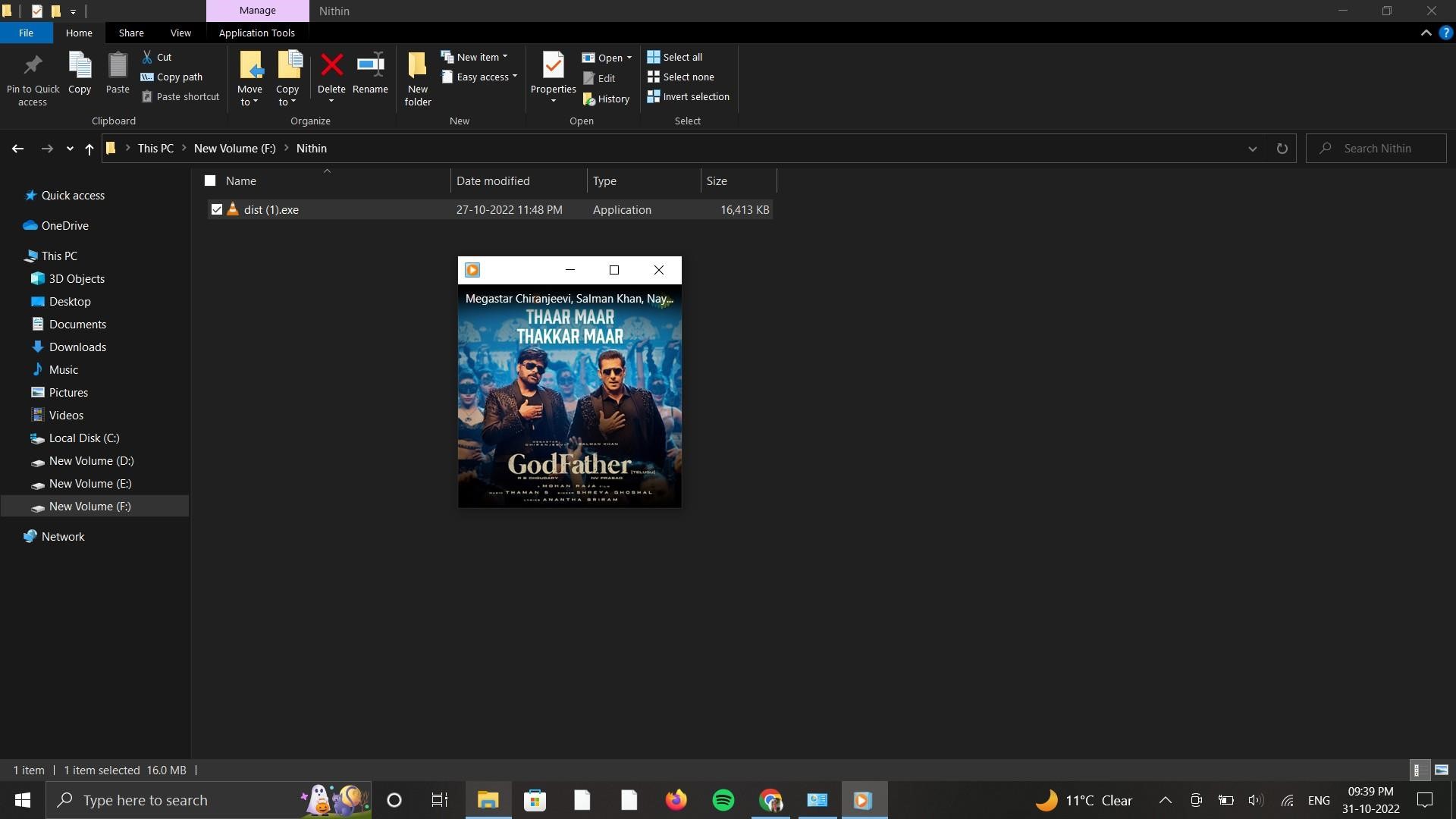


We created an exe file which contains the audio file and payload with an icon of VLC media player.

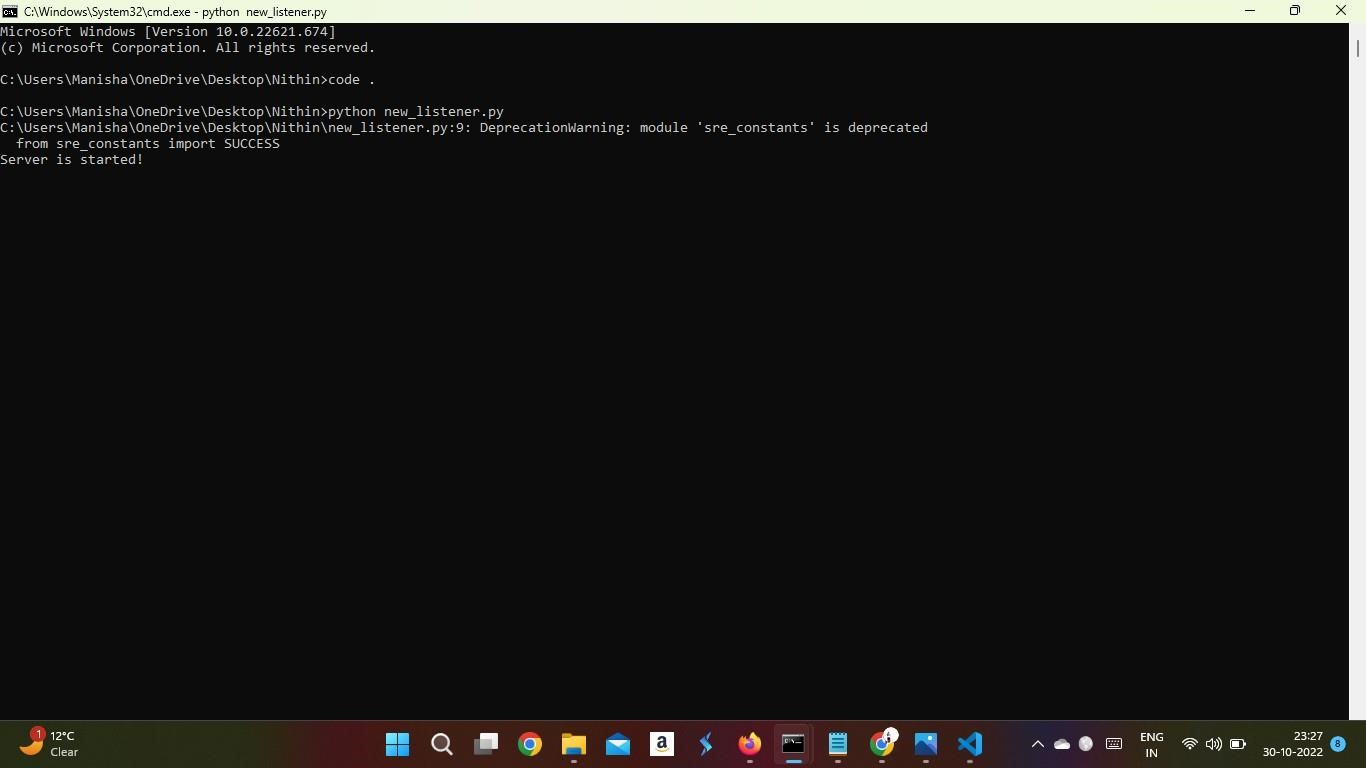
Once the victim executes the exe file, the inserted file is played along with the attacker gaining access to the victim’s computer.



Once the dist.exe isexecuted we can see that the music player gets poppedup and it plays the music but in background we get the access to the victim computer.

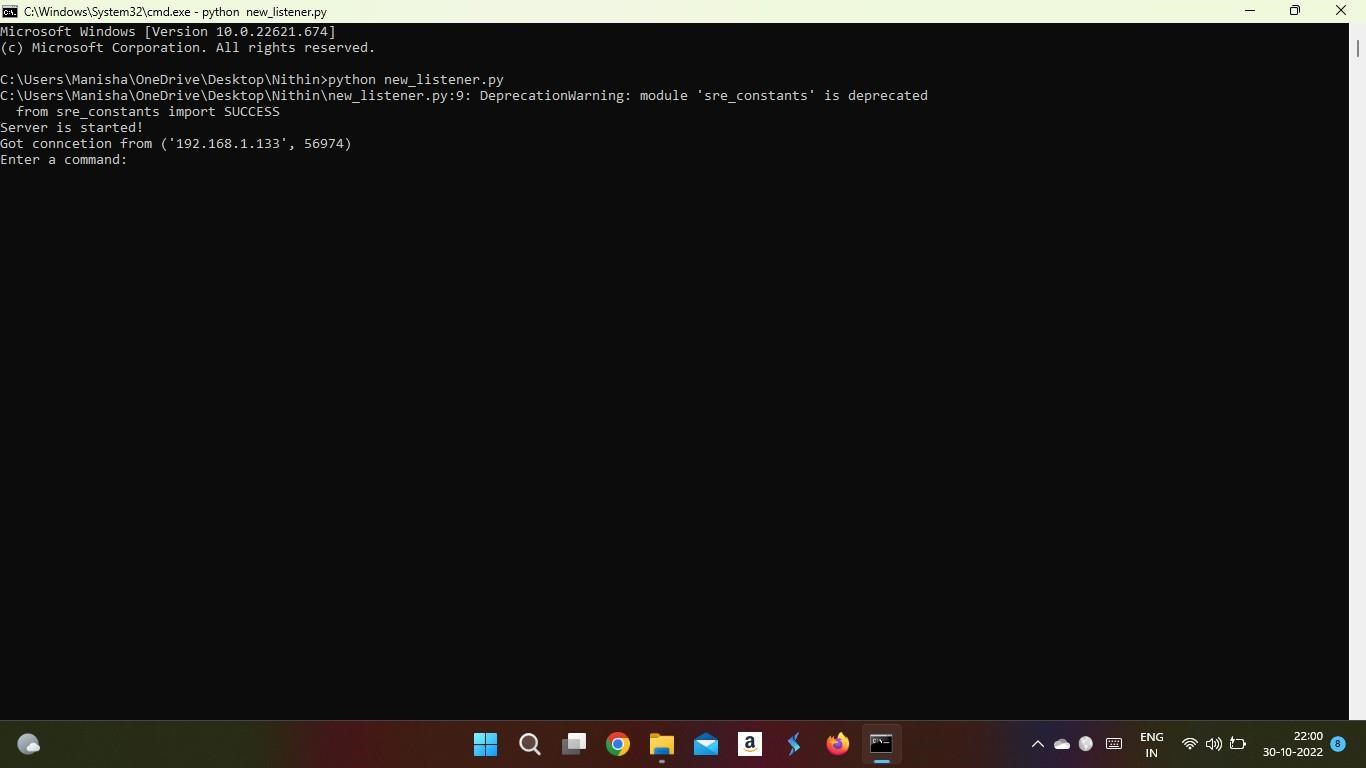


Here new\_listener.py is the listener program, once the program is executed the program will be up and listens for any incoming connections that are available stating Server is started!



When the Payload isexecuted on the victim computer the connection will beestablished and we will receive the response from the computer with the IP address of the victim computer.

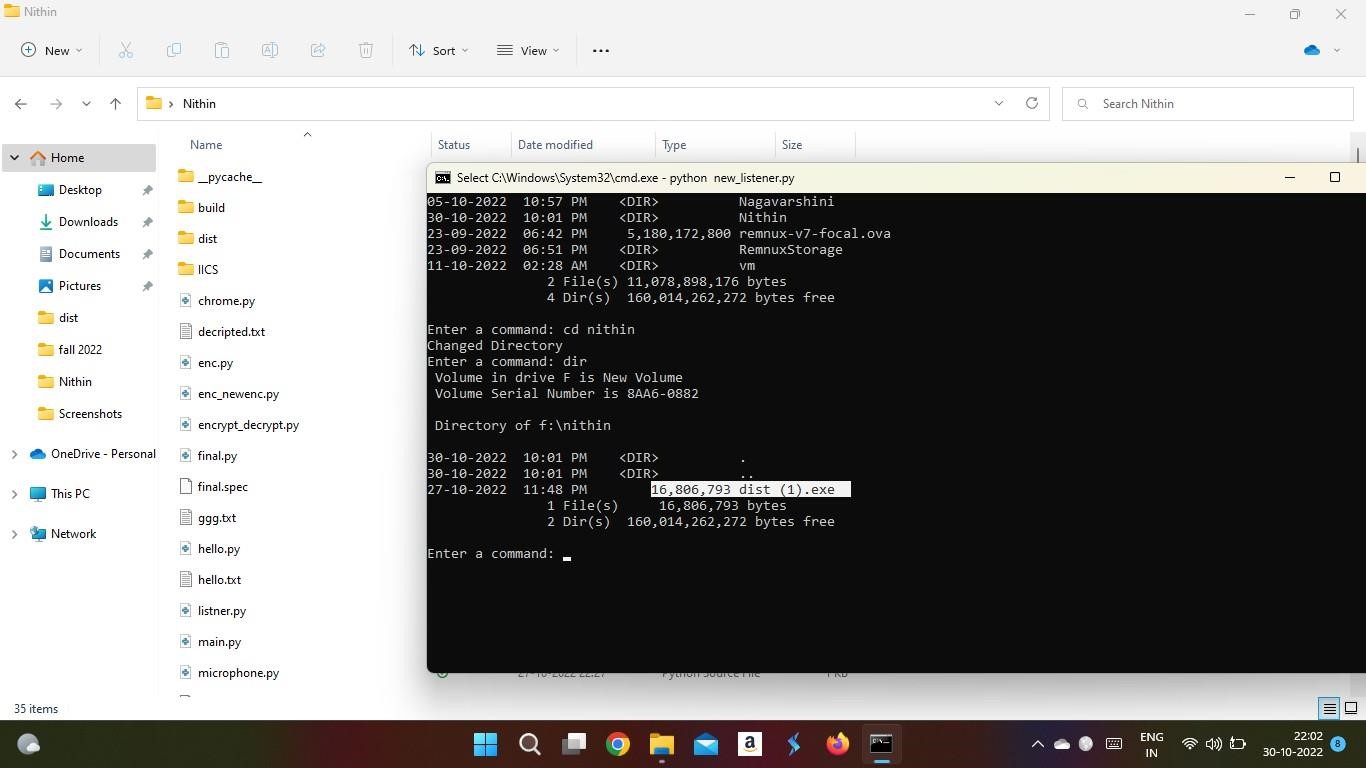
Here the victim IP-Address is: 192.168.1.133



Once the connection is established, we can execute all the commands from the attacker computer to get them reflected in the victim computer.

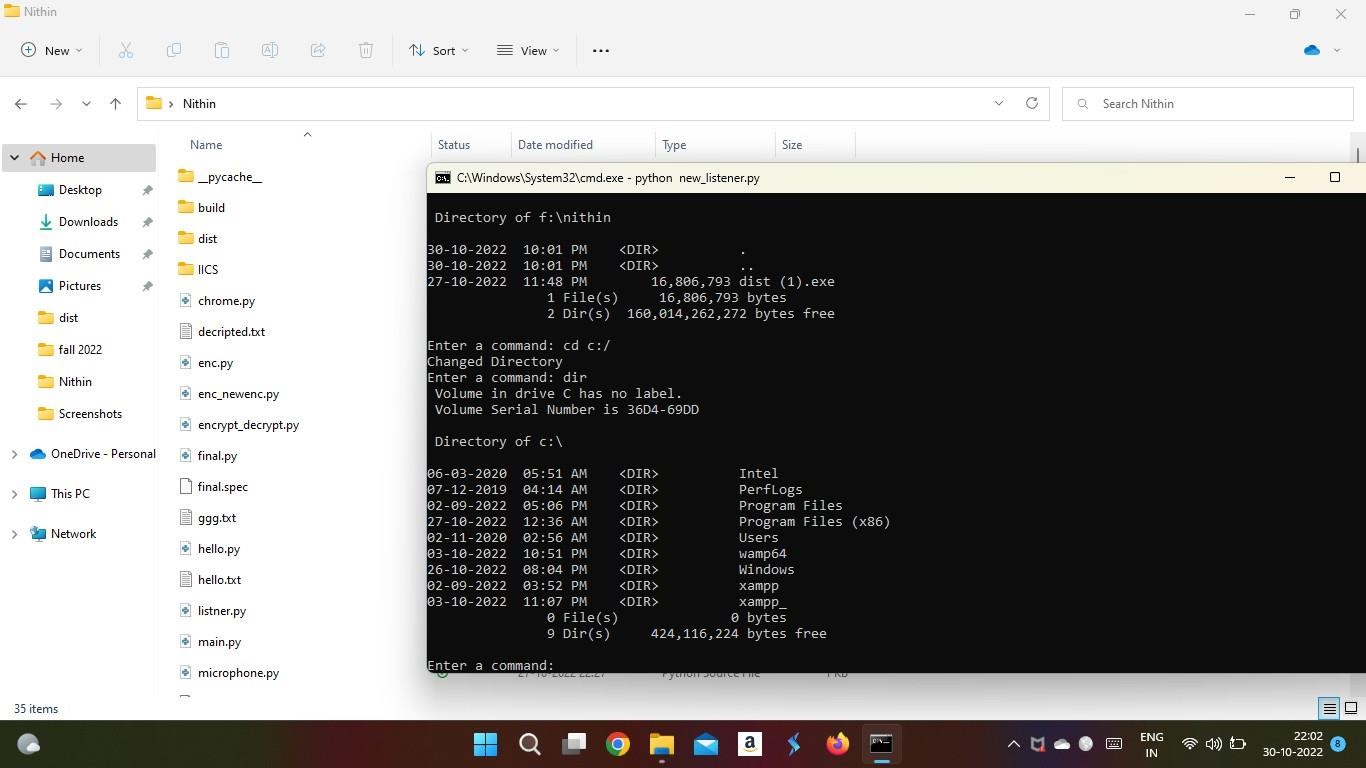
When dir command is executed, we can see the result of the victim computer.

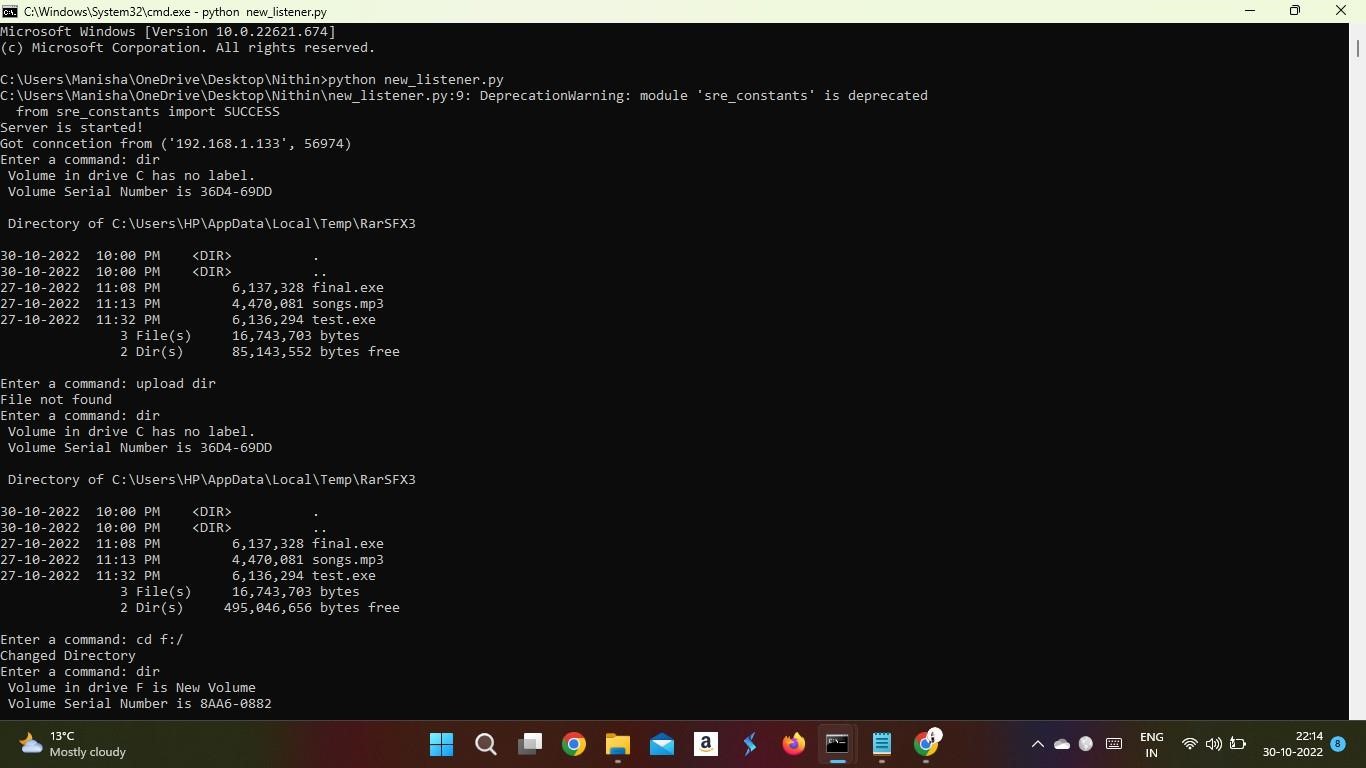
Now we have deleted all the files to erase the attacker’s traces from victim’s computer. We can see that the file is empty now, it only has mydist.exe which is a payload.

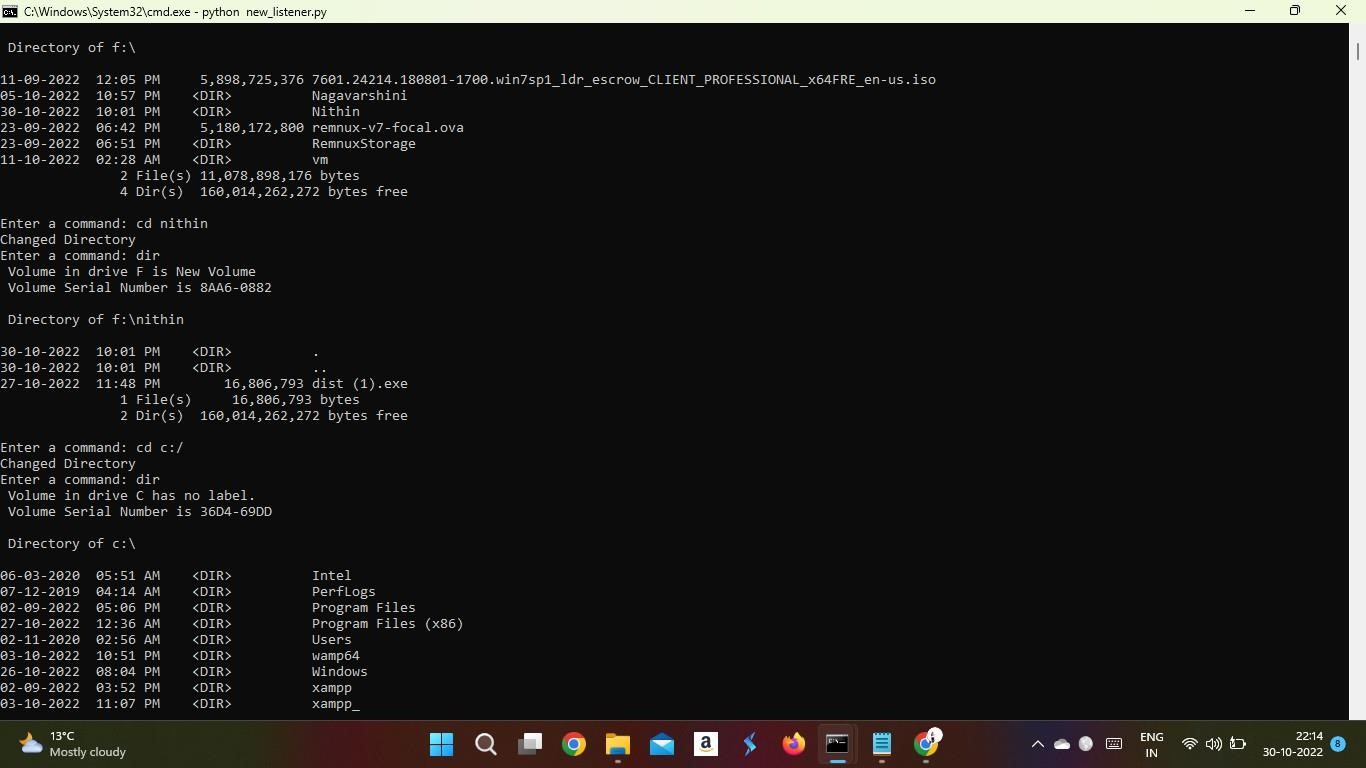


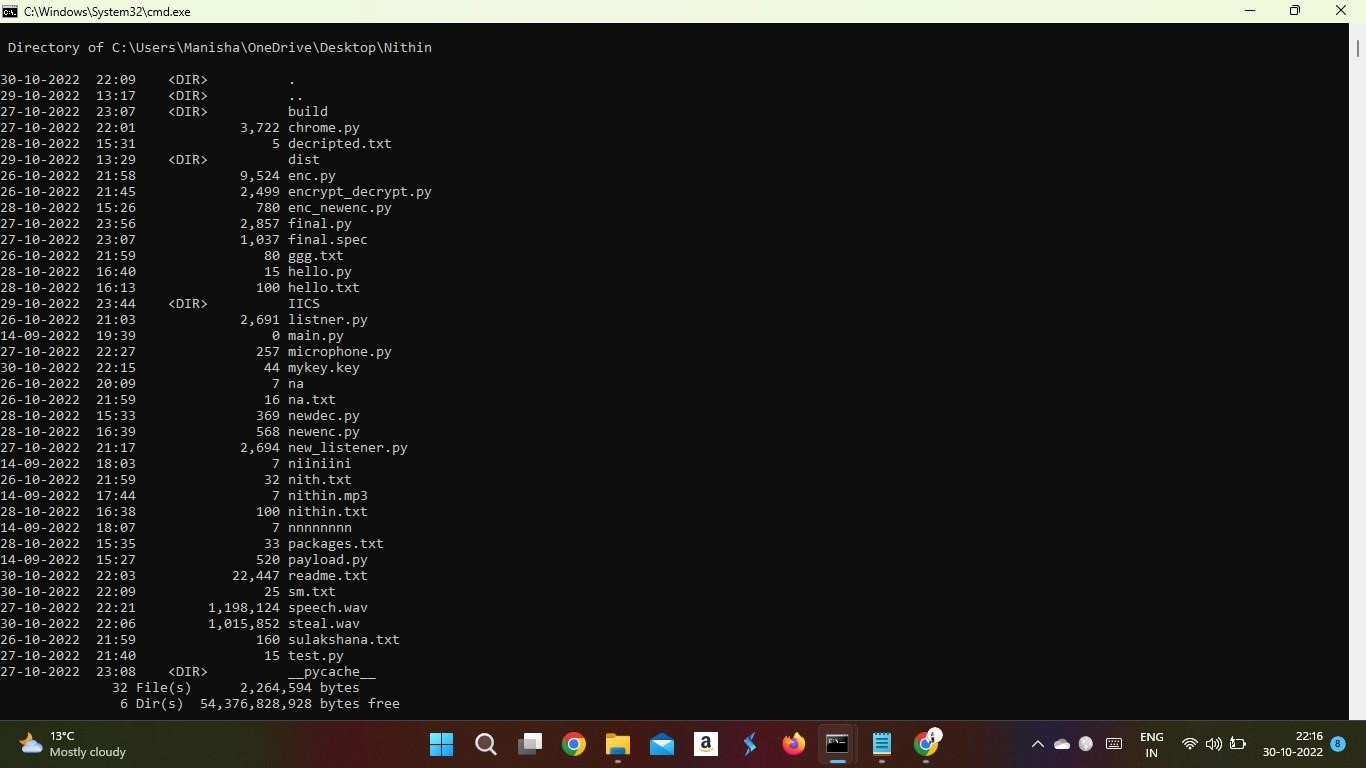
**Accessing the Victim’s File system**

We accessed the file system of the victim’s computer to check the available files. And the attacker can modify any files he wants.









**Team member’s contribution:**

We executed three features in this round which are developed by each team member.

**Venkat Nithin Atturu**:

Developed the payload and listener programs and embedded the payload into the mp3 file in which the mp3 is embedded to the exe with a VLC icon and developed a program to steal all the information of the victim that is stored in Google Chrome on the victim’s computer such as bookmarks and passwords.

**Nagavarshini Surapaneni:**

Developed the payload and listener programs, and the programs to encrypt and decrypt the files of the victim computer. Tested the developed encryption and decryption programs on the victim’s computer by encrypting victim’s files and decrypting them.

**Sulakshana Mucheli:**

Developed the other feature of this round that is accessing the microphone of the victim computer, and storing the recorded audio to the file, and actively participated in the project for the successful implementation.

**Features developed in this Project for accessing victim’s computer information are**

* Extracting saved passwords from Google chrome on victim’s computer
* Accessing microphone of the victim’s computer
* Encrypting and Decrypting files on victim’s computer
* Extracting system level information of victim computer