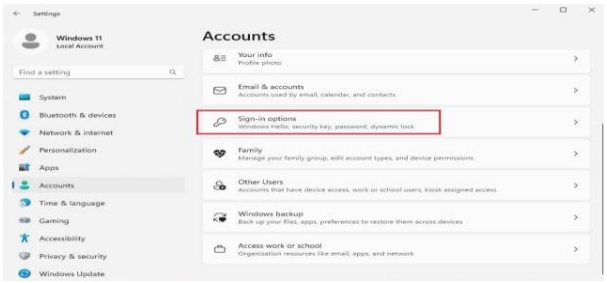
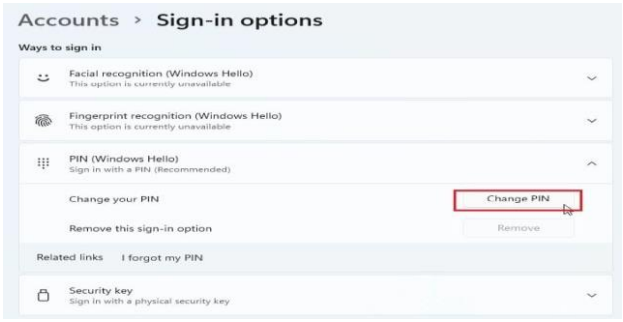
**1) Change/set windows desktop security pin/ password & check windows update system**

❖ **Password setup or change pin**

- Step1:- press the windows 11 keyboard shortcut “windows + I” to open the setting app. Now, move to accounts-> sing-in option.




- Step2:-here click to expand the “password” section and then click the “change pin” button.




- Step3:-after that enter the current password of your windows 11 pc and click on “next”.


- Step4 :- on the next page, you can change the password easily. You can also add a hint to help you recover your account in case you forget the password.

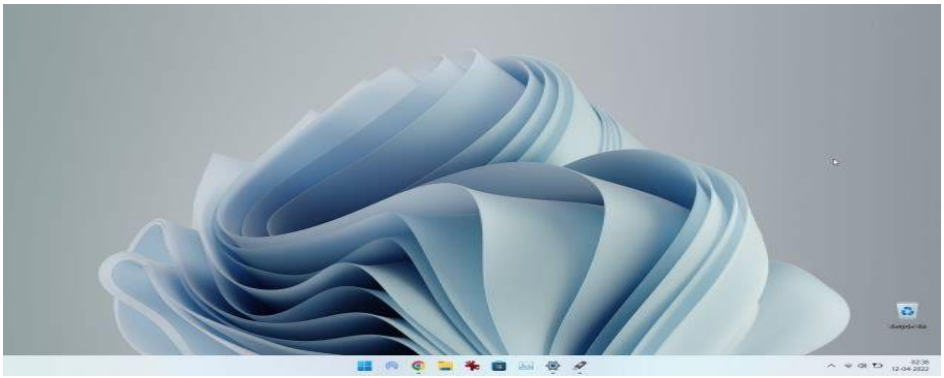

- Step5 :- finally click on “finish”, and you are done. You have successfully changed your windows 11 password.

### ❖ Check windows update and update the system

- Step1:- first press the windows 11 keyboard shortcut “windows + I ” to open the settings app. Next, navigate to the “windows update” section from the left sidebar.

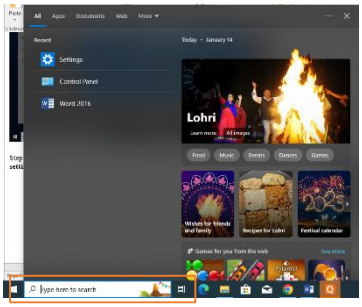

- Step2 :- once here, click on “check for updates”. If there is an update available, it will show up here and will be downloaded automatically.


- Step3 :-after that the update will be installed, and you will be asked to restart your pc. Simply reboot Your windows 11 pc in no time.

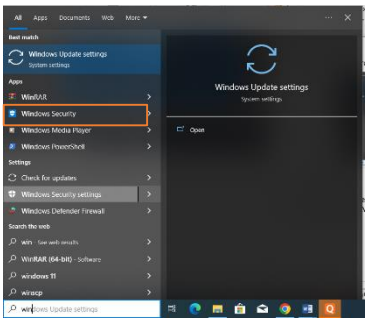


## 2) Demonstrate Turn on & off Windows OS Firewall

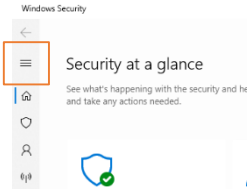
- **Step 1: go to search**



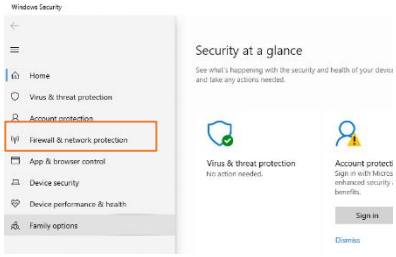

- **Step 2: search windows security**



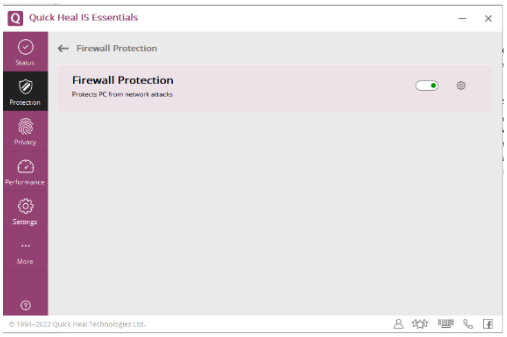

- **Step 3: Click on Navigation button**




- **Step 4: Click on Firewall and network protection**




- **Step 5 :- if you installed any anti-virus software's the firewall will open in app , now you can on & the firewall**

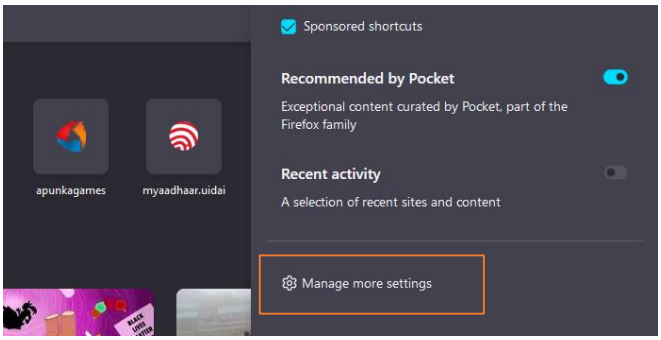


### 3) Check the browser and website certificates and analyze the certificates

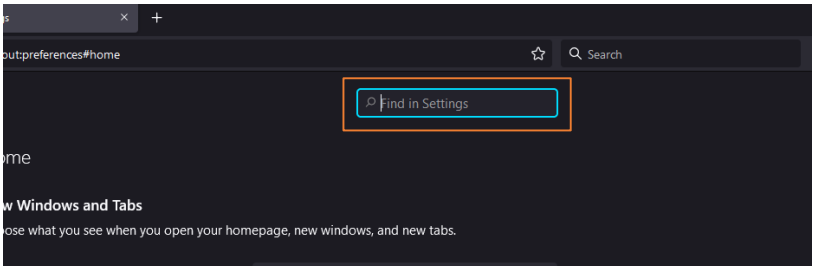
#### ❖ Browser certificates view

- Step 1:- Open Firefox Browser and click on settings icon

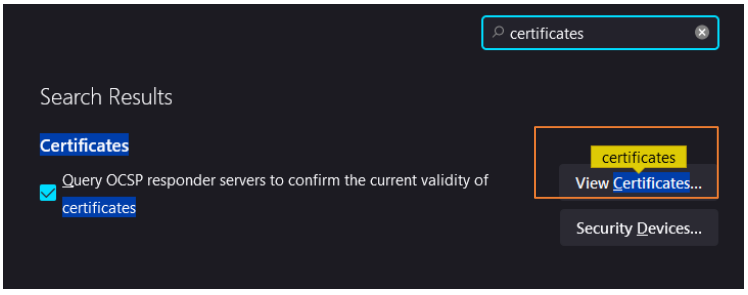

- Step 2:- click manage more setting option



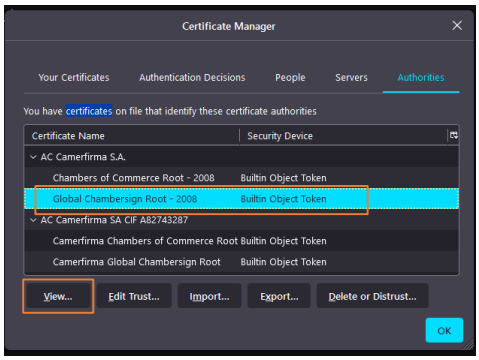

- Step 3:- Search certificates in search box




- Step 4:- Click on view certificates



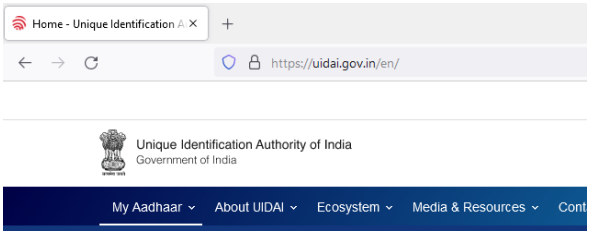

- Step 5:- Select any one certificate and click view



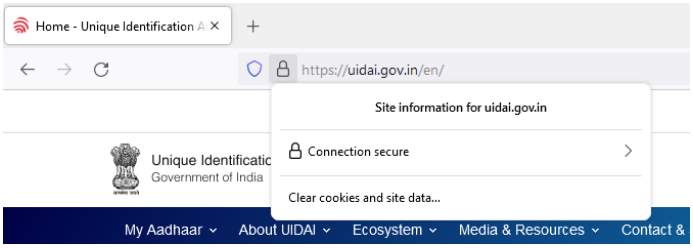

- Step 6:- Now you can see the certificate

### ❖ Website certificate check

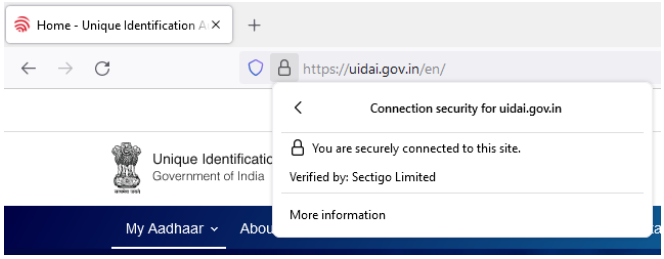
- Step 1:- Goto firefox and search any website
- Step 2:- Click lock icon on left side top corner



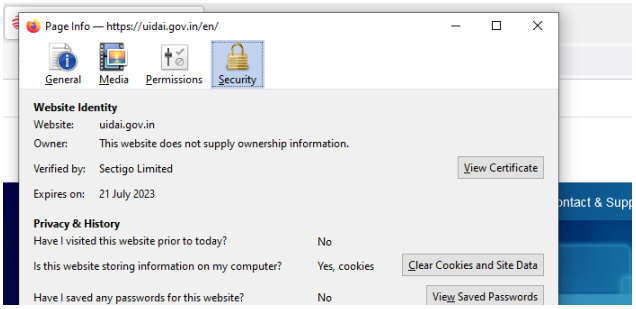

- Step 3:-Click connection secure



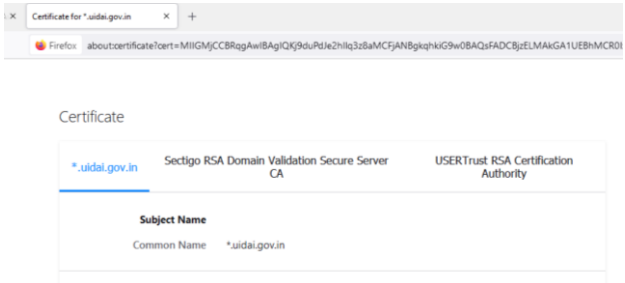

- Step 4:- Click more information




- Step 5 :- Now click view certificate

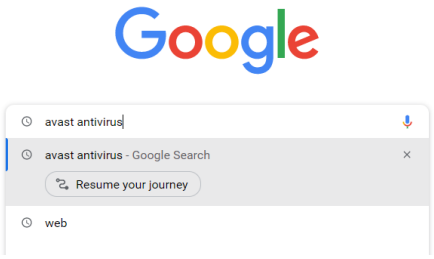



- Step 6:- Now you can see the certificate details

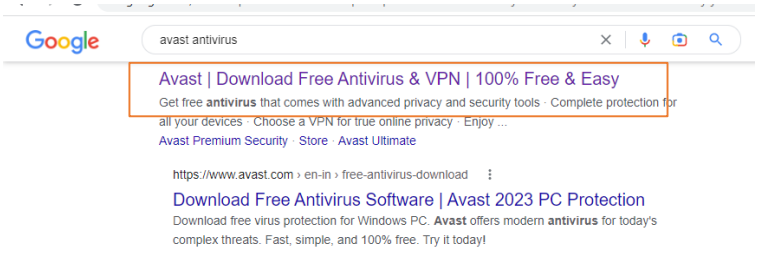


**4) Install Anti-virus and scan the computer.**

- Step 1:- Open any browser and search avast antivirus.

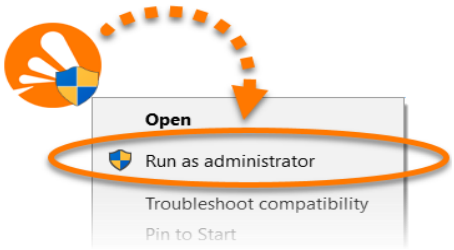



- Step 2:- click on avast download free antivirus & vpn link

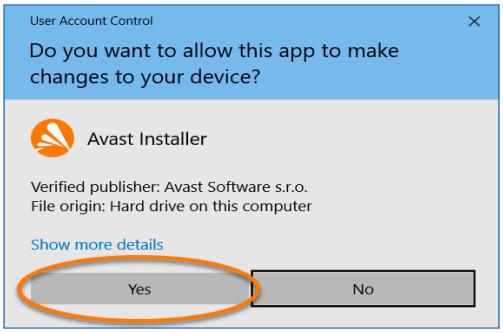



- Step 3:- click on Download free protection button

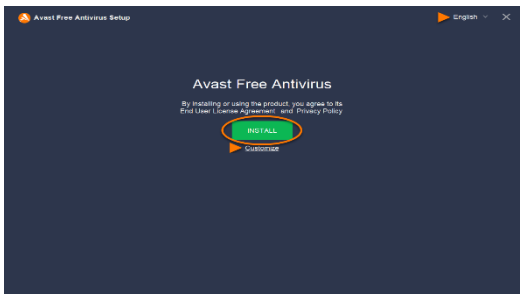

- Step 4 :- Right-click the downloaded setup file and select Run as administrator



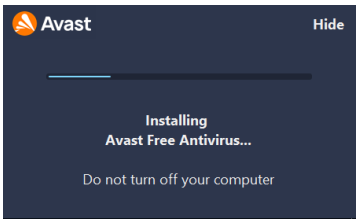

- Step 5: If prompted for permission by the User Account Control dialog, click Yes.



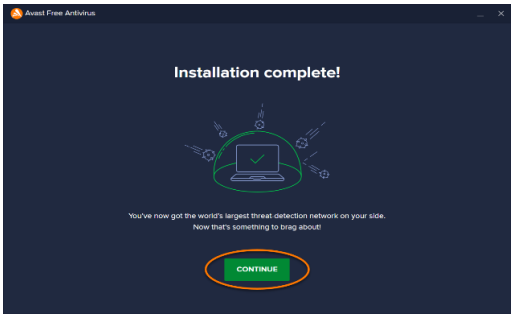

- Step 6: Then, click Install



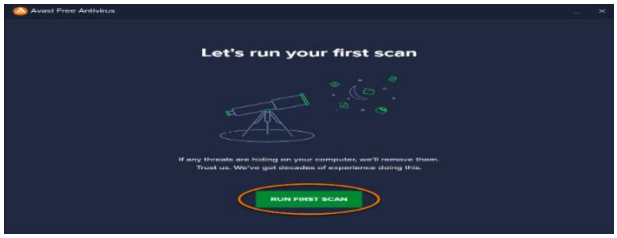
- Step 7: Wait while setup installs Avast Free Antivirus on your PC.




- Step 8:When the installation is complete, click Continue.




- Step 8:Click **Run first scan** to start a comprehensive Smart Scan,



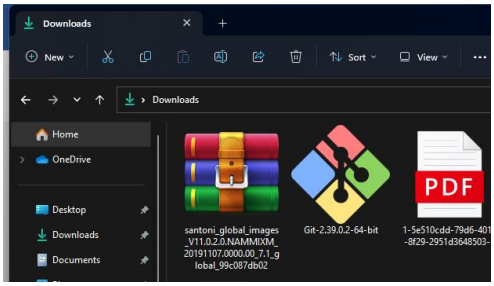
**5) Install Git app and perform the basic git operations below**

- ❖ Create a repository
- ❖ Cloning a repository
- ❖ Making and repository changes
- ❖ Viewing the history of all changes

➢ Step 1: Browse to the official Git website: https://git-scm.com/downloads

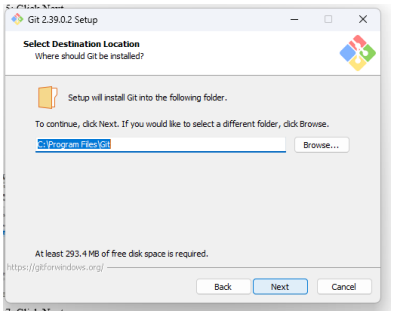
➢ Step 2: Click the download link for Windows and allow the download to complete.


➢ Step 3: Double-click the file to extract and launch the installer.

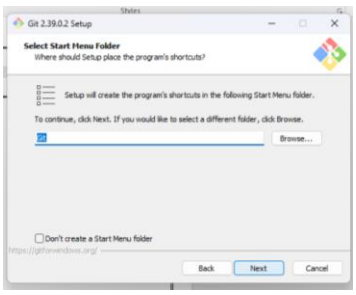



➢ Step 4: Click Next.

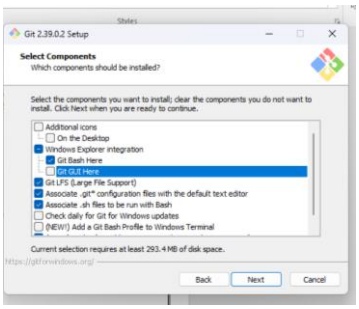

➢ Step 5: Click Next.



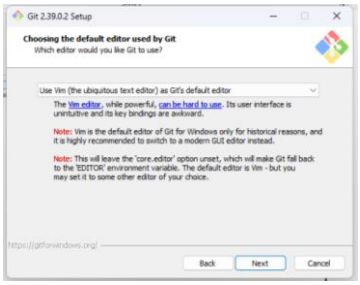

➢ Step 6: Click Next.



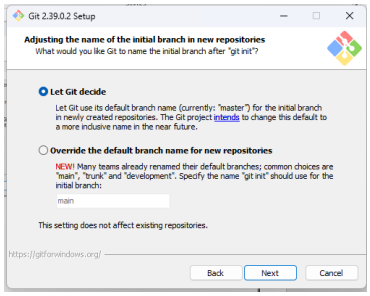
- Step 7: Simply click Next.



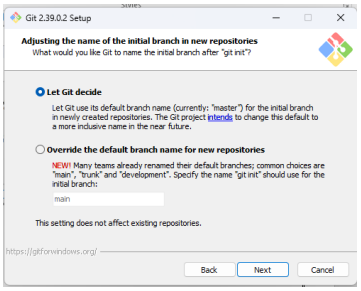

- Step 8: Click Next.



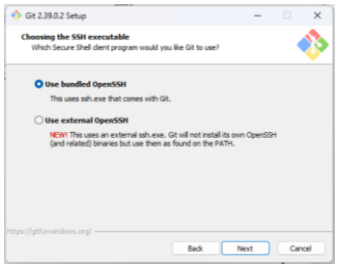

- Step 9: Click Next.



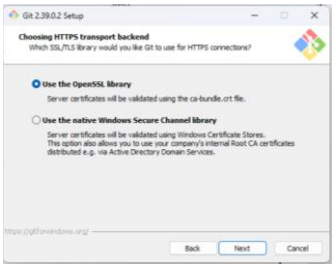

- Step 10: Click Next.



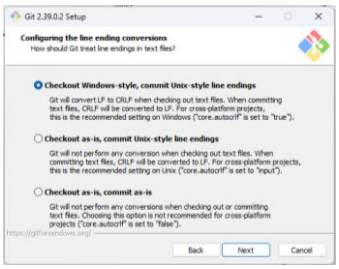

- Step 11: Click Next.



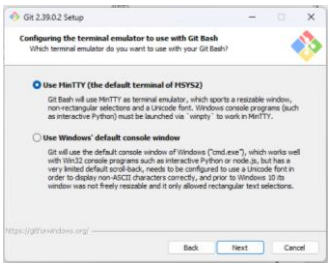

- Step 12: Click Next.



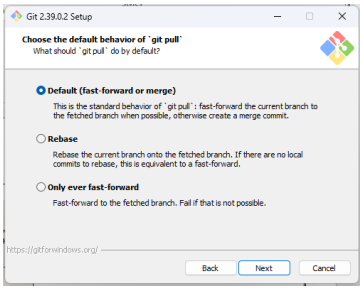
- Step 13: Click Next.



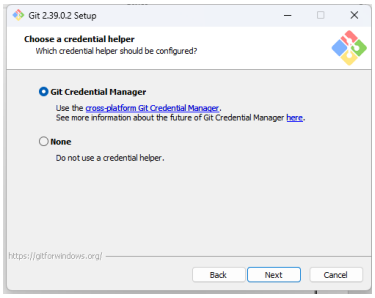

- Step 14: Click Next.



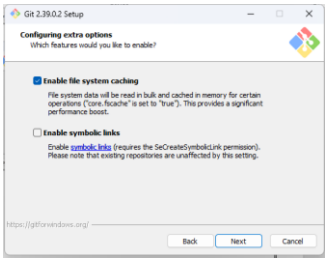

- Step 15: Click Next to continue with the installation.



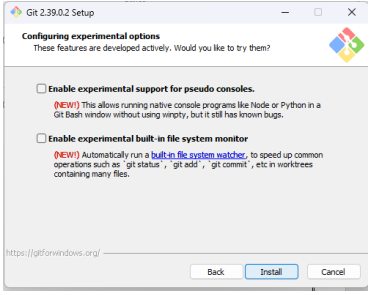

- Step 16: Click Next.



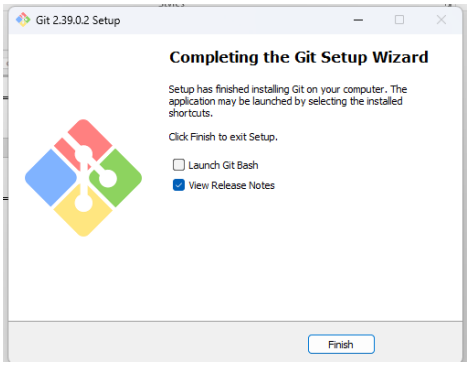

- Step 17: Click Next.




- Step 18: Click Install.



- Step 19: Click Finish.




**basic git operation**

- Create a repository
  Git init command is used to create a repository (master)

- Cloning a repository
  Git branch CS command create a repository as master knows as clone

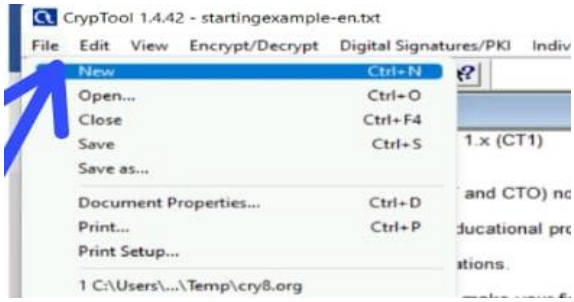
- Making and repository changes
  Git commit -m "my recent changes" it is used to making changes.

- Viewing the history of all changes
  Git status it is used to view the history of changes,

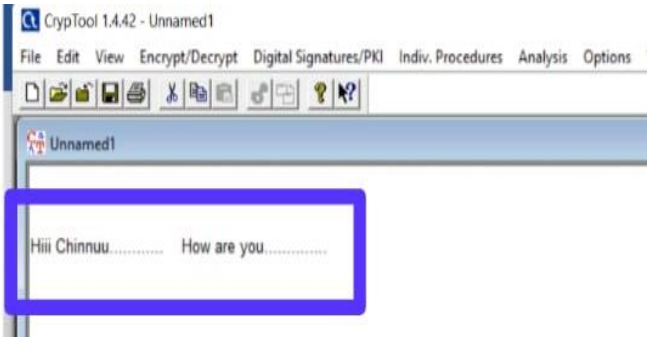
**6) Design a simple crypto system [encryption, decryption, digital signature] using any crypto tool**

❖ **Steps for Encryption**

➢ **Step 1: -** Go to file & Click on the new in crypto tool

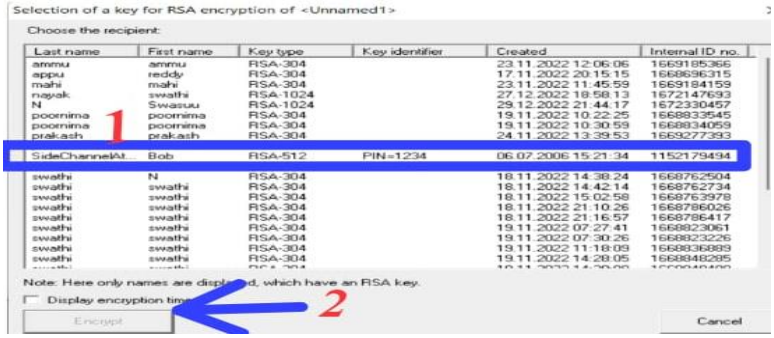



➢ **Step 2: -** Then type the message

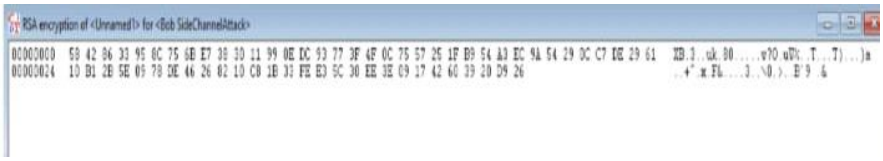



➢ **Step 3: -** Go to Encryption/Decryption option & Select asymmetric Then Click on the RSA encryption


➢ **Step 4: -** Choose the recipient & Double click on the recipient Then click on the encryption



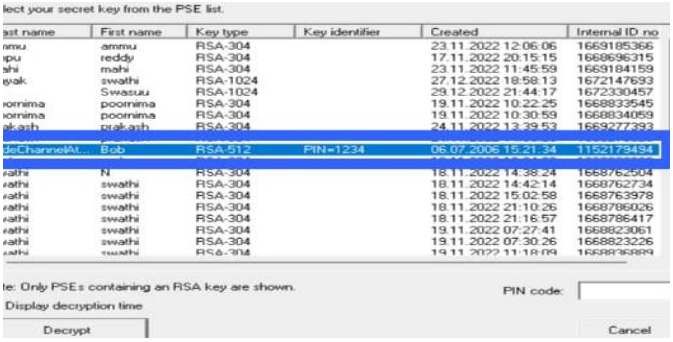
➢ **Step 5: -** Then your message will be encrypted



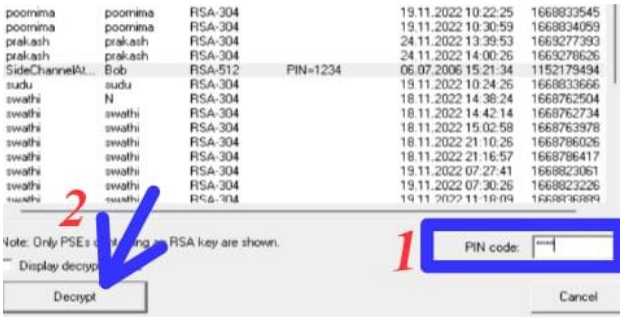

❖ **<u>Steps for Decryption</u>**

➢ **Step 1: -** Go to Encryption/Decryption & Select the asymmetric Then click on the RSA decryption

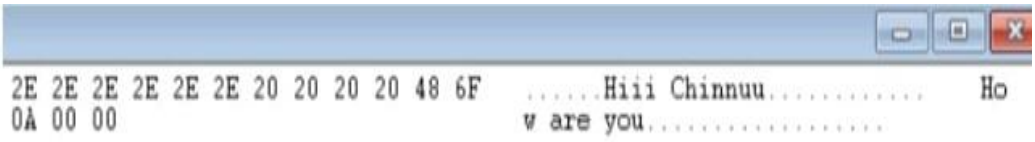

➢ **Step 3: -** Select your secret key from the PSE list Then double click on the PSE




➢ **Step 4: -** Enter the PIN code Then click on the Decrypted

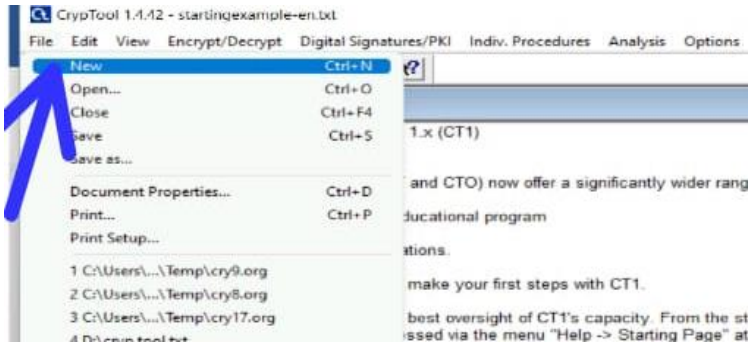



➢ **Step 5: -** Then your message will be decrypted

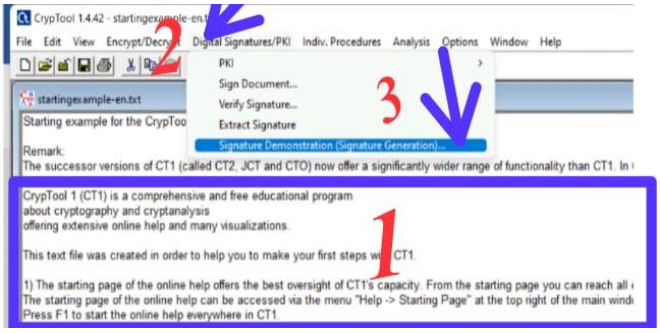


## ❖ Steps for Digital Signature

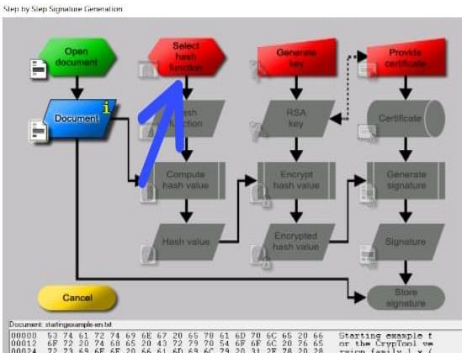
➢ **Step 1: -** Go to file Then click on the new



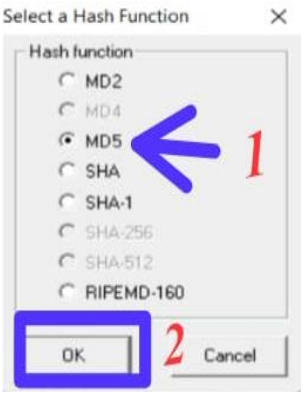

➢ **Step 2: -** Type the message & go to digital signature Then click on the signature demonstration



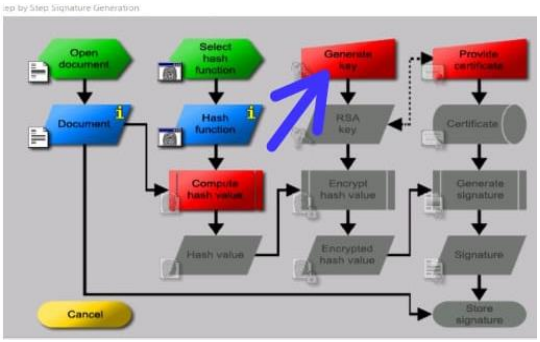

➢ **Step 3: -** Click on the select hash function



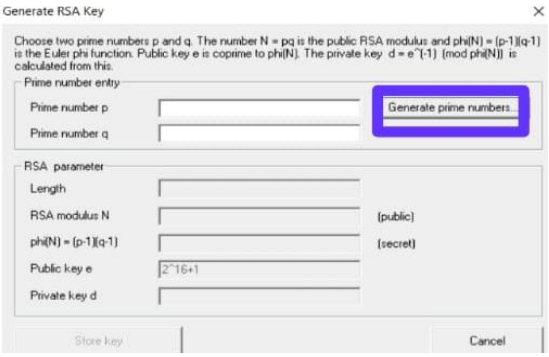

➢ **Step 4: -** Click on MD 5 Then click on ok option



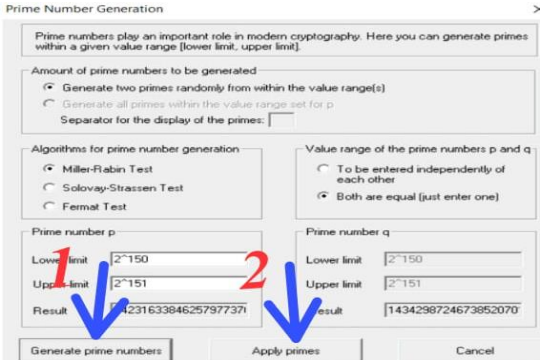
➢ **Step 5: -** Then click on the generate key



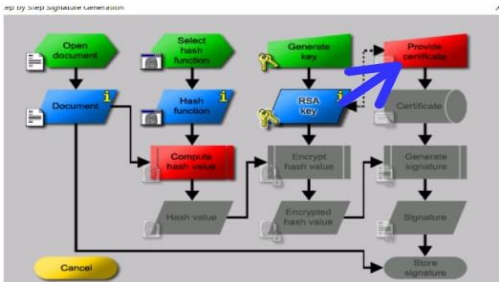

➢ **Step 6: -** Click on the generate prime numbers



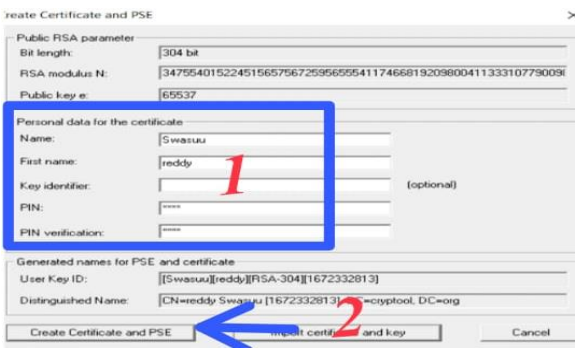

➢ **Step 7: -** Select on the generate prime num Then click on apply primes




➢ **Step 9: -** Click on the provide certificate

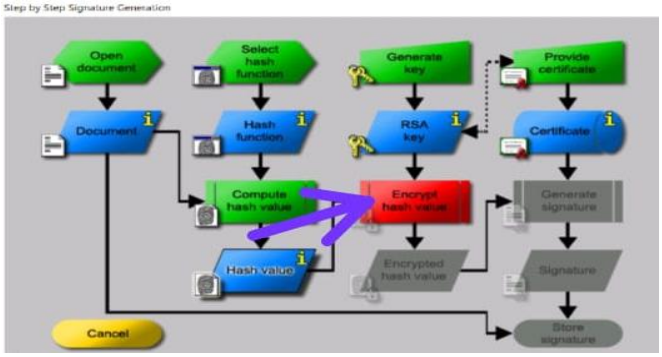



➢ **Step 10: -** Create your PSE certificate Then click on the create certificate PSE

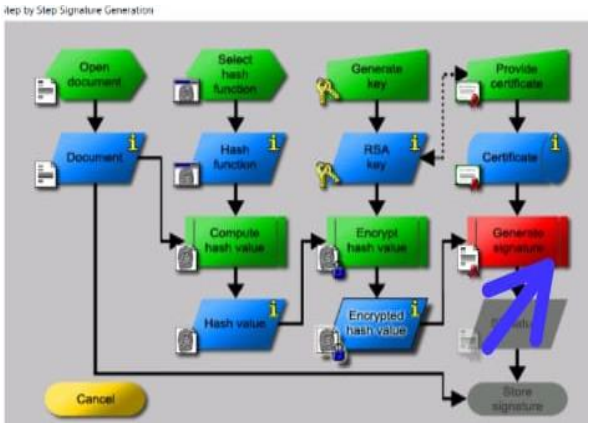


- **Step 11: -** Then click on the compute hash value

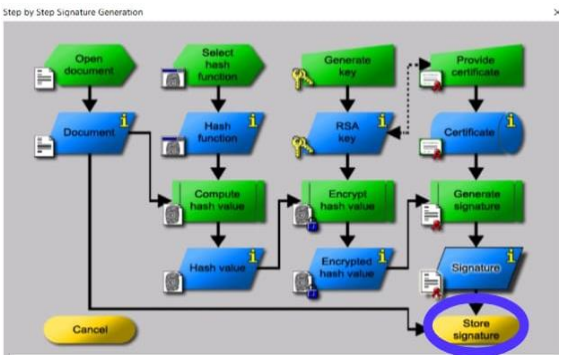

- **Step 12: -** Click on the encrypt hash value




- **Step 13: -** Then click on the generate signature

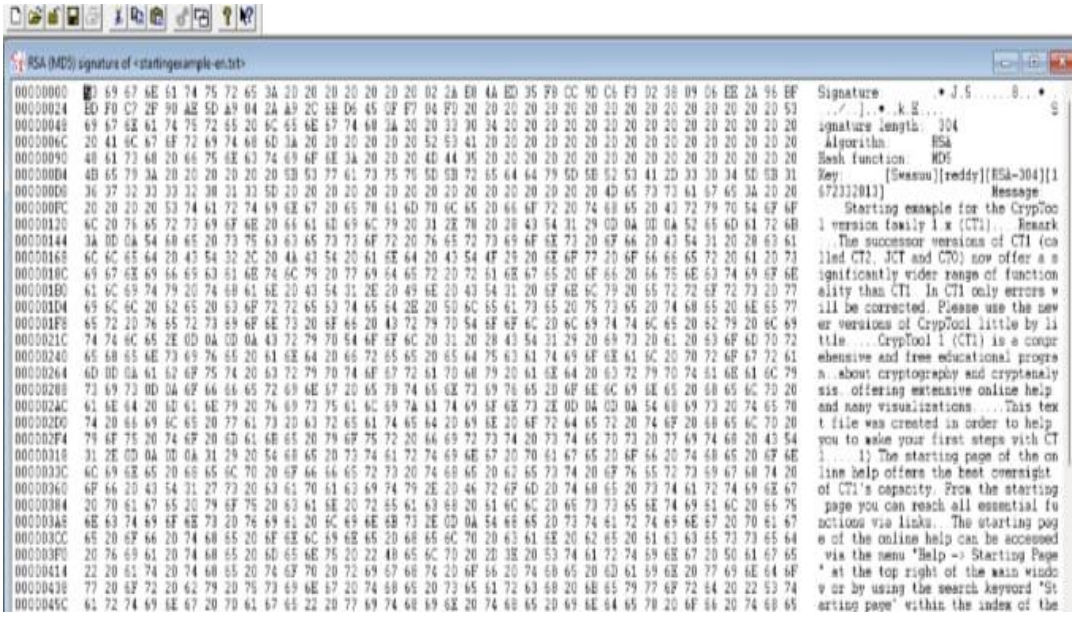



- **Step 14: -** Click on the store signature



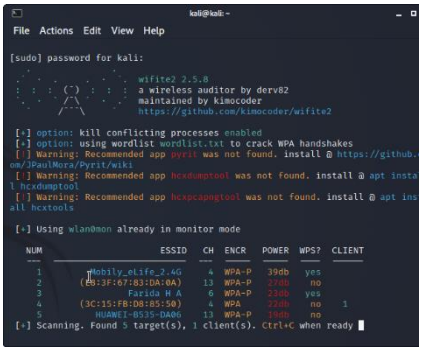
- **Step 15: -** Shows the results Then click on ok option


- **Step 16: -** digital signature will be displayed on the screen.

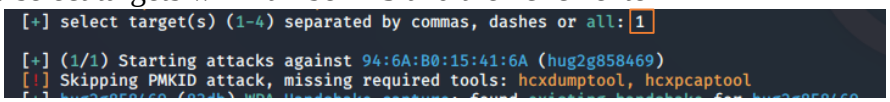


## 7) Crack a WIFI Password using wifite

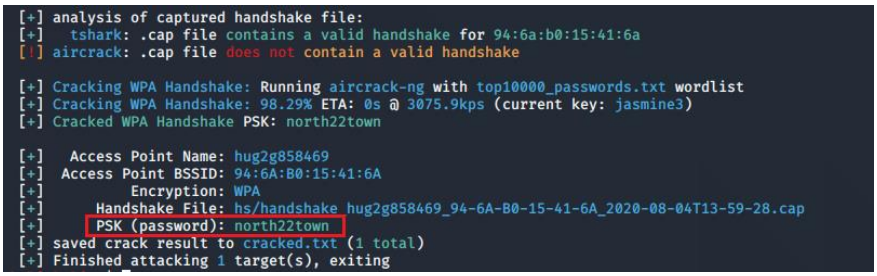
- Step 1:- Go to terminal in kali Linux and type this command **"sudo wifite"** and press enter
- Step 2:-The wifi scanning will begin wait untill your wifi will show then press ctrl+c




- Step 3:- Now select targets wifi number 1-5 and then click enter



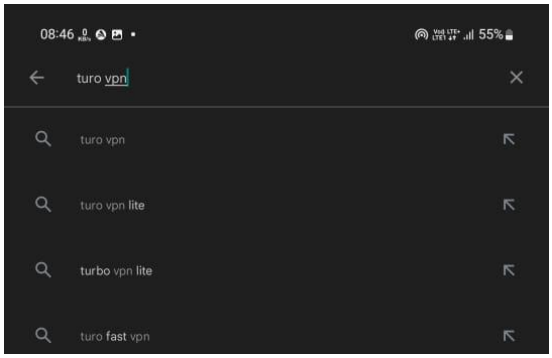

- Step 4 :- Wait until password crack then you can see the wifi password



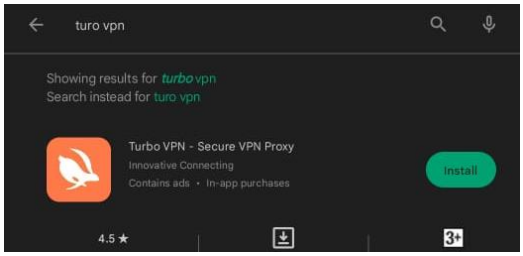
**8) Install VPN on mobile and pc and check connection**

❖ **On Mobile**

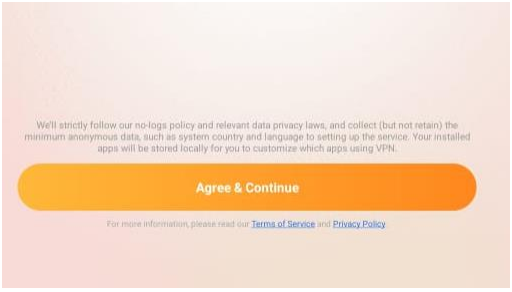
- step 1:-open Playstore and search turbo vpn



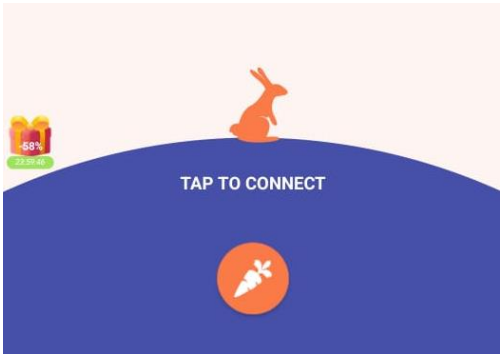

- Step 2:- click install



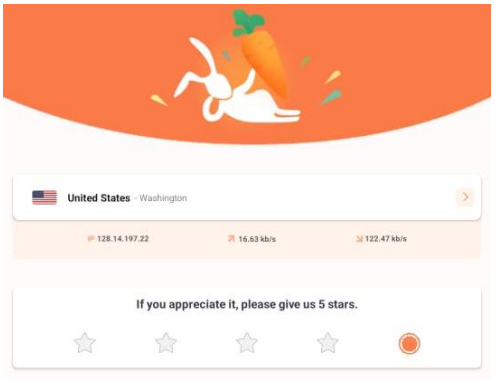

- Step 3:-open turbo vpn and click agree & continu




- Step 4:- press tap to connect



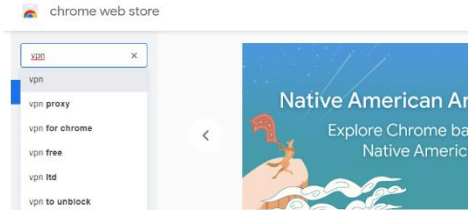

- Step 5:- vpn connected succfully



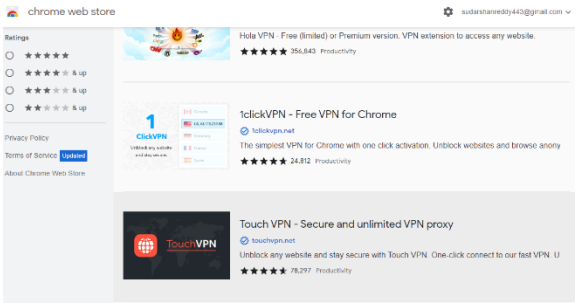
## ❖ On Computer

- Step 1:- open chrome browser and search “https://chrome.google.com/webstore”

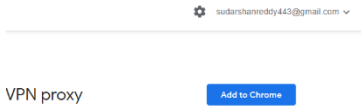

- Step 2:- search vpn on webstore



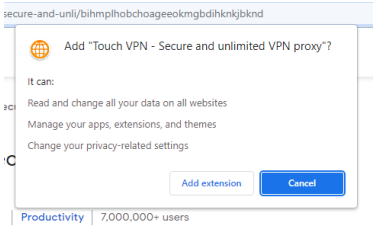

- Step 3:- Click any one vpn



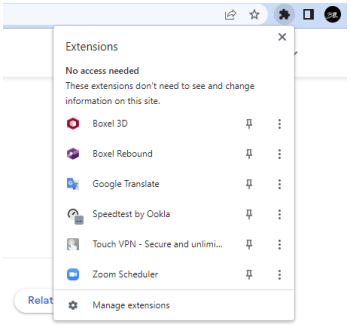

- Step 4:- click add to chrome button to install vpn



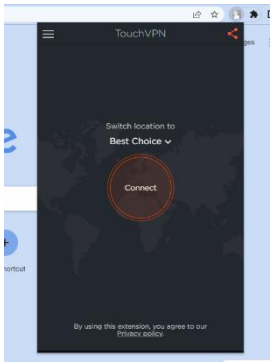

- Step 5:- Click add extension to confirm



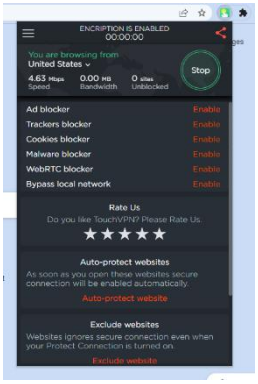

- Step 6:- Click extension icon and click downloaded vpn



- Step 7:- select server and click connect

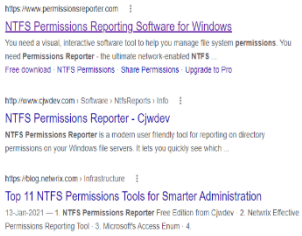



- Step 8 :- vpn connected succsfully \



**9) Demonstrate NTFS file system using NTFS permission reporter.**

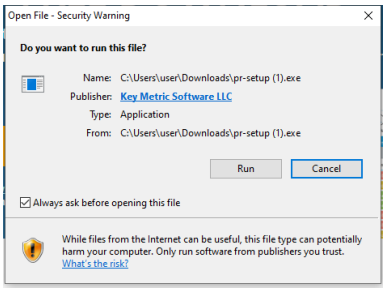
- **Step 1**: open any browser, search for NTFS file permission reporter



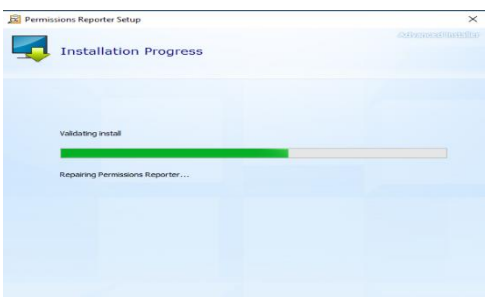

- **Step 2**: Click on Download Now


- **Step 3**: Click on Start Download

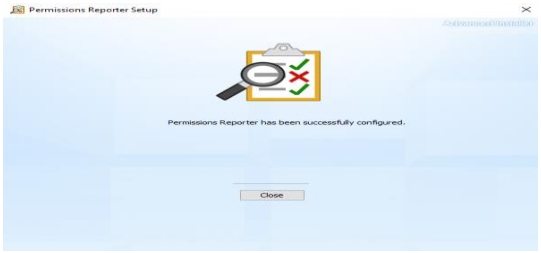

- **Step 4**: Click Run



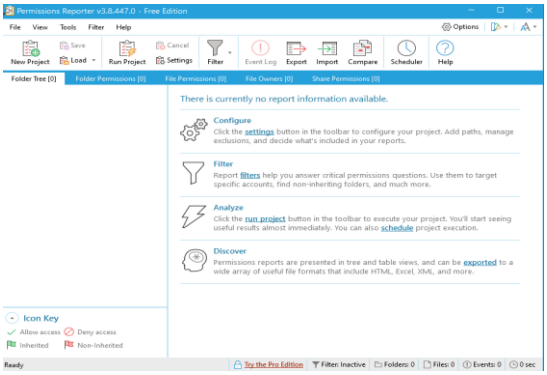

- **Step 5:** Click on Next

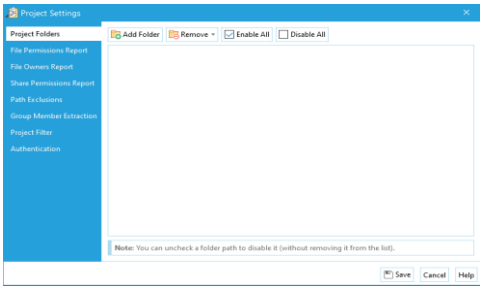
- **Step 6**: Click on Close

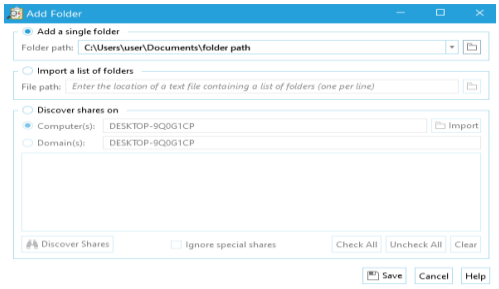



- **Step 7**: open the permission reporter
- **Step 8:** In Configure, Click on settings

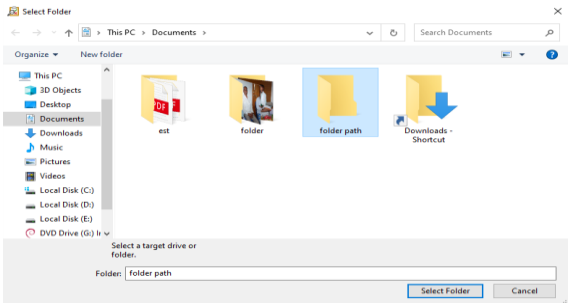



- **Step 9:** In project settings, Select Add Folder

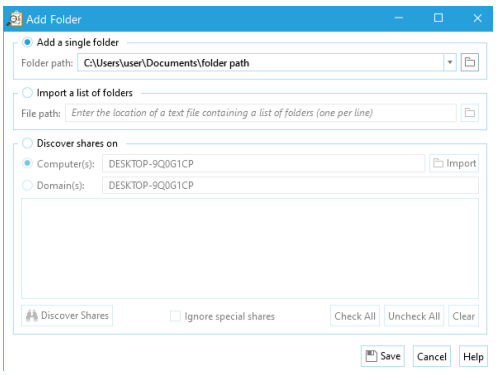


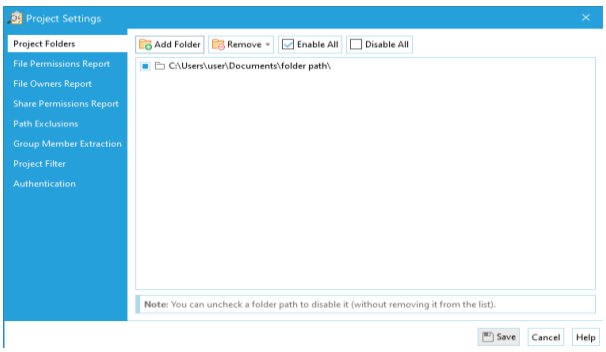

- **Step 10:** Select the folder and Click on Select Folder



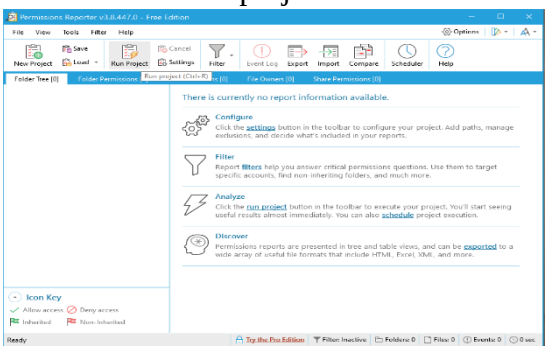

- **Step 11:** Click on Save



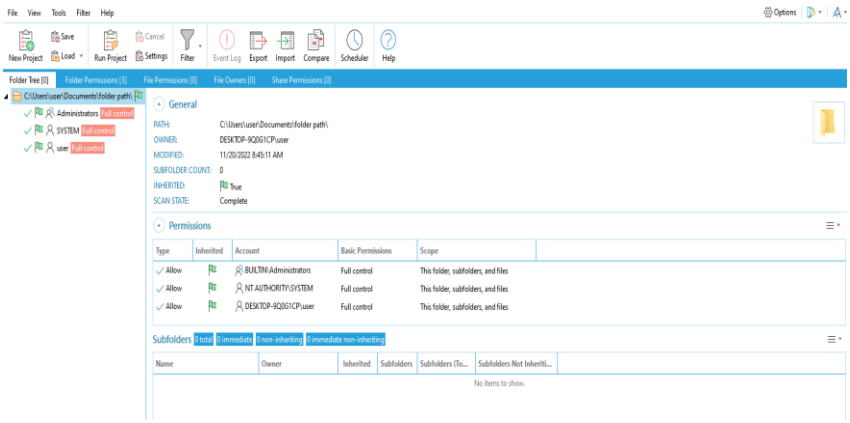
- **Step 12:** Click on Save




- **Step 13**: Click on the run project

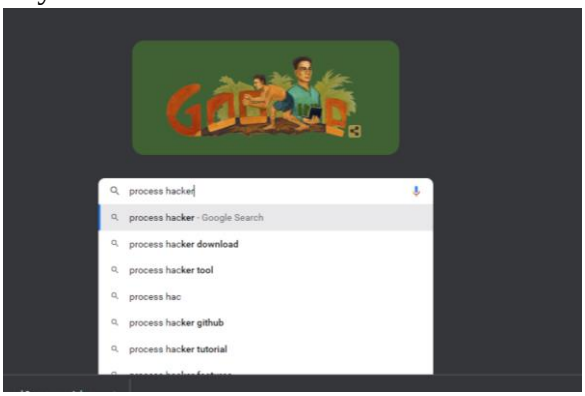



- **Step 14** : permission of the select folder display on the screen



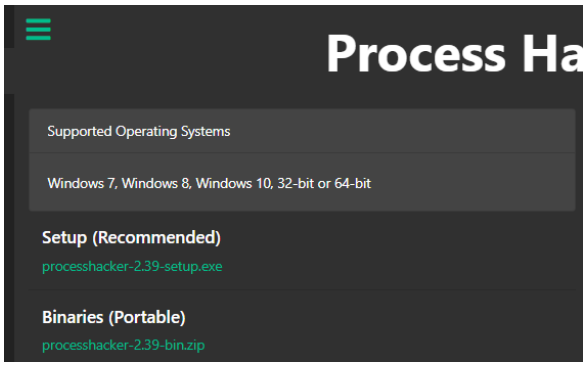
## 10) Installation of process hacker and observe the process with all details.

- **Step 1: -** Go to any browser & Search Process Hacker

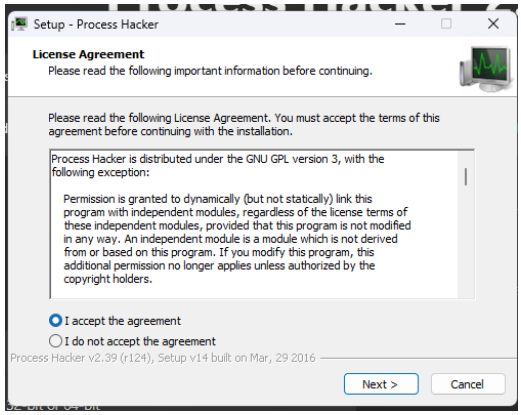



- **Step 2: -** Search the download process hacker

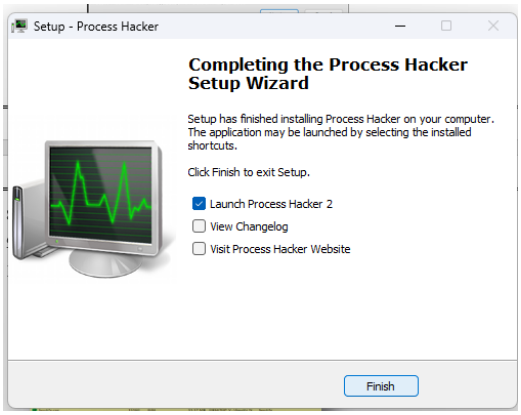

- **Step 3: -** Then click on the process hacker – 2.39-setup



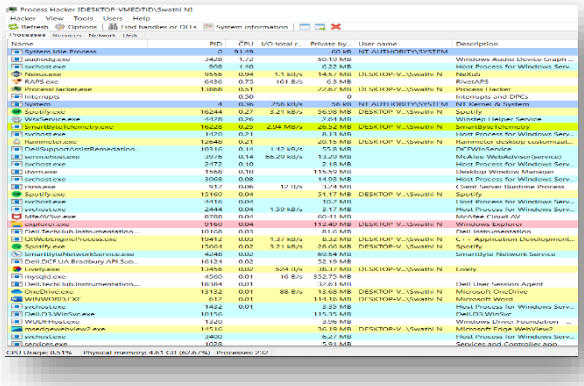

- **Step 4: -** Process hacker will be downloaded
- **Step 5: -** Then process hacker will be displayed on the screen
- **Step 6: -** Double click on the process hacker
- **Step 7: -** Then click on yes option and click on the next



- **Step 8: -** Then click on the Install
- **Step 9: -** Click on the finish button

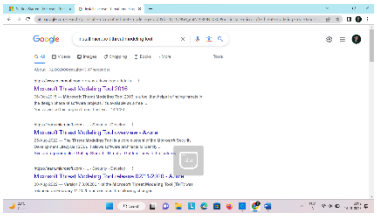



- **Step 10: -** Then you can observe the process with all details

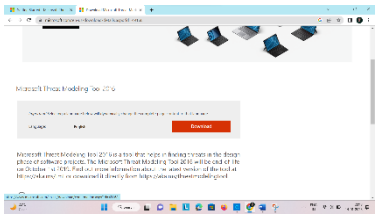


**11) Using the Microsoft threat model software, create a threat model for any application architecture.**

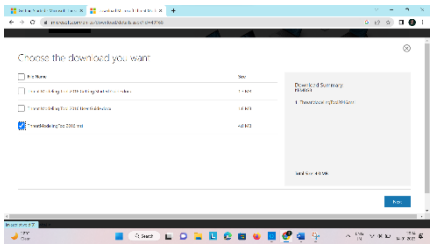
- **Step 1** go to any browser search Microsoft threat Modeling tool download



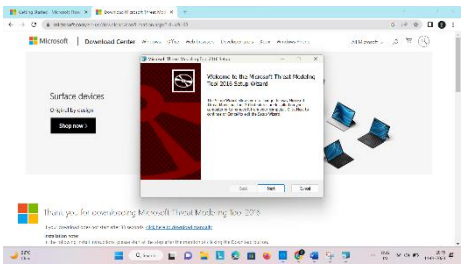
- **Step2** Display the screen Download Microsoft threat Modeling tool 2016



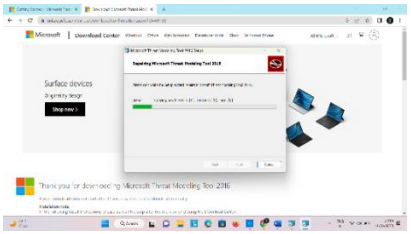
- **Step 3** Choose the download you want ThreatModelingTool2016.msi 4.0 click Next



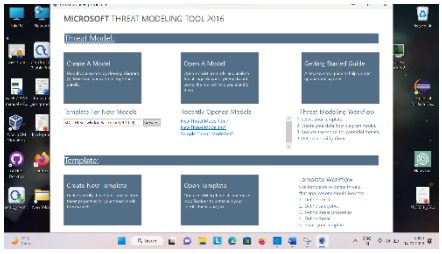
- **Step 4** Click Next



- **Step 5** finish the installation click next step

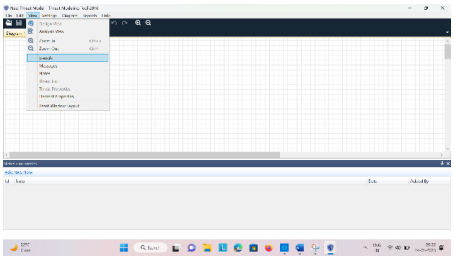


- **Step 6** After installation completed go to Threat Model create A Model

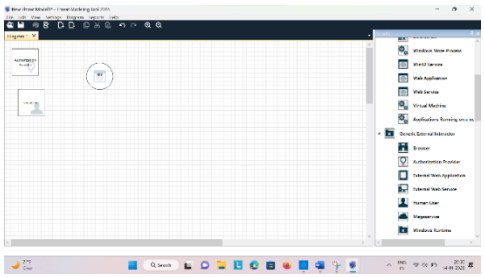


## Create application

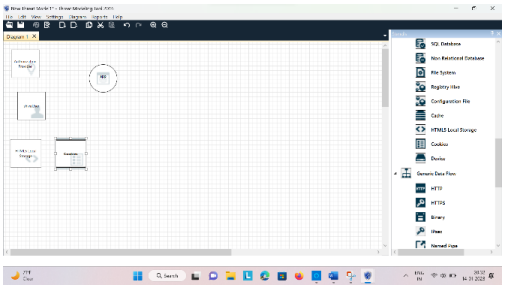
- **Step 7** go to view click stencils display the tools



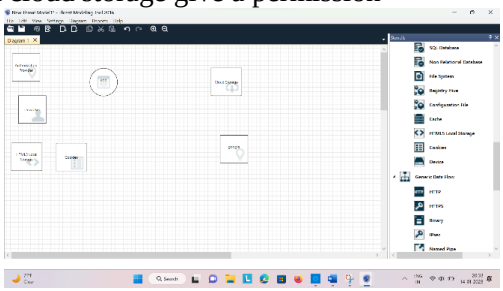
- **Step 8** Take application, Human user, Authentication provider and give the permission



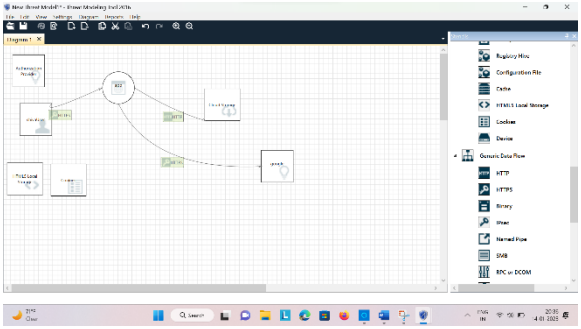
- **Step 9** Take local storage HTML and security cookies



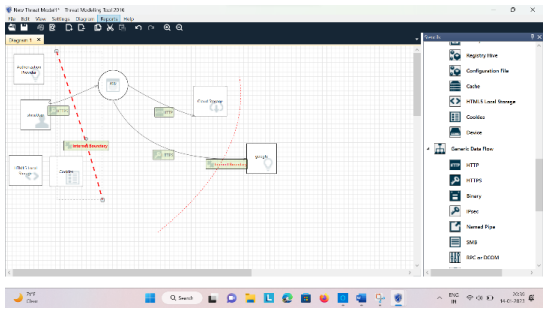
- **Step 10** Take browser and cloud storage give a permission



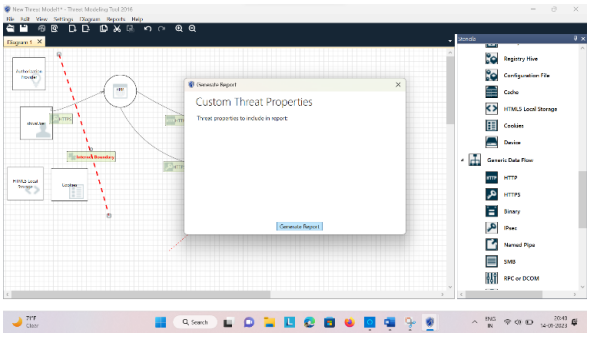
- **Step 11** Assign HTTPS user, google to app and HTTP app to storage



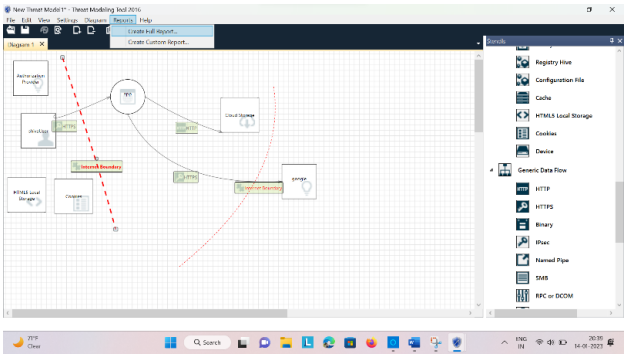
- **Step 12** Add Internet Boundary and got reports



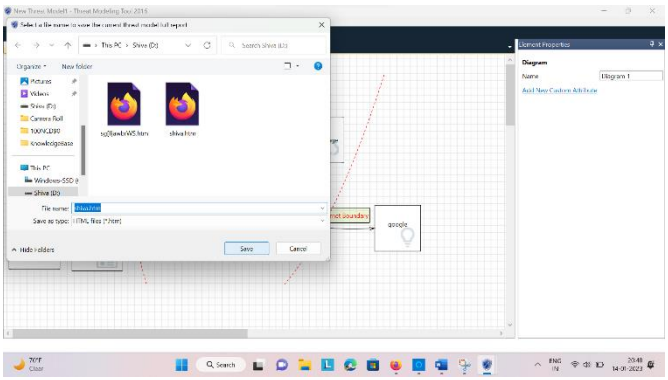
- **Step 13** Click Create Full Report




- **Step 14** Threat properties to include in report , Generate Report



- **Step 15** Save the file and view the report

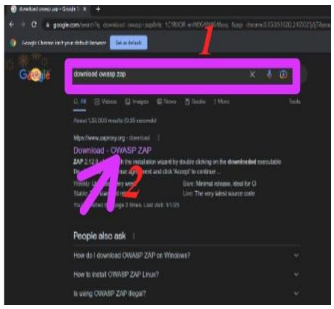


- **Step 16** Report will be generated find the vulnerability and threat in your application

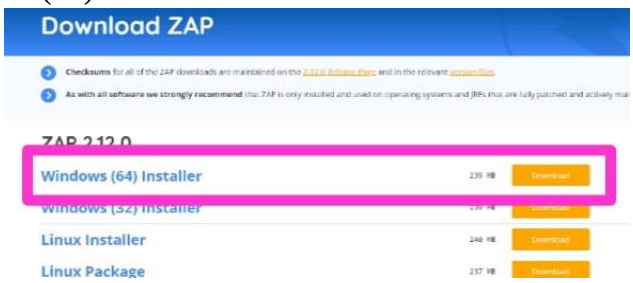
**12) Install OWASP ZAP and demonstrate finding vulnerabilities in web application using automated scan & Manual Scan.**

*** Automated scan:**

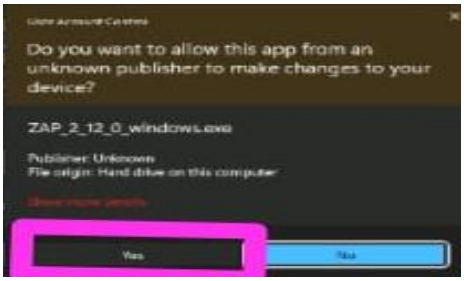
- Step 1: - Go to chrome & search the download OWASP ZAP then click on the download – OWASP ZAP



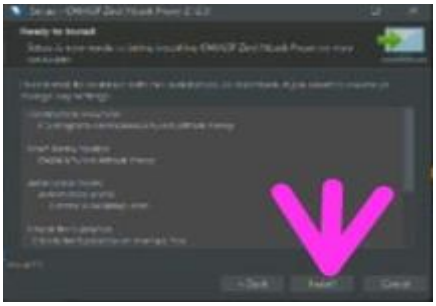

- Step 2: - Select windows (64) installer 239MB then click on the Download




- Step 3: - Now ZAP will be downloaded & double click on ZAP then click on yes



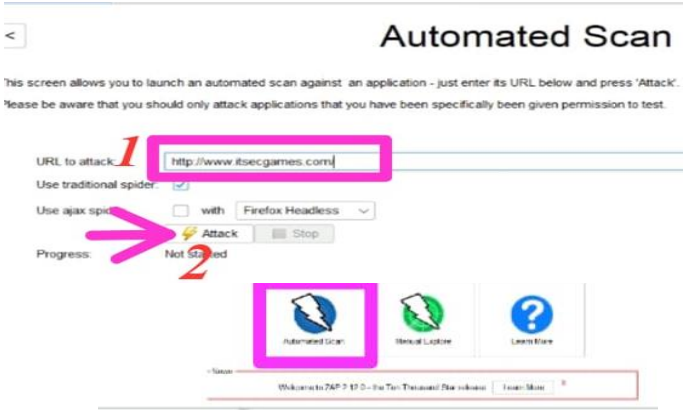

- Step 4: - Click on the next... next… next… next… then click on install option



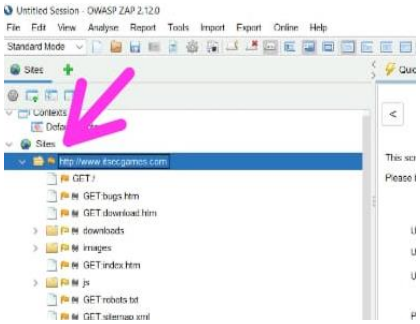
- Step 5: - Then click on the finish button

- Step 6: - Open the OWASP ZAP then click on the Automated scan

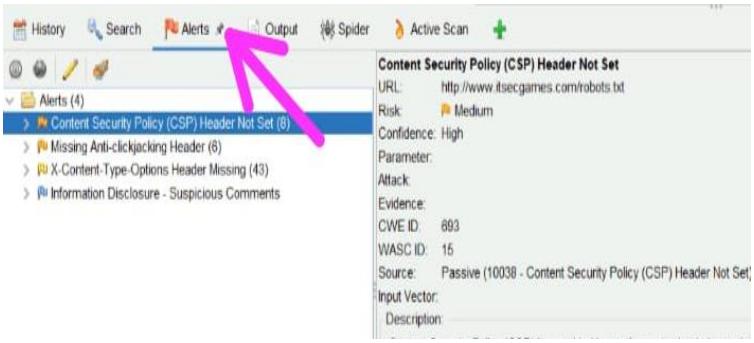
- Step 7: - Paste BW app website URL then click on attack button




- Step 8: - Click on sites for different files in that and analyze request and response header

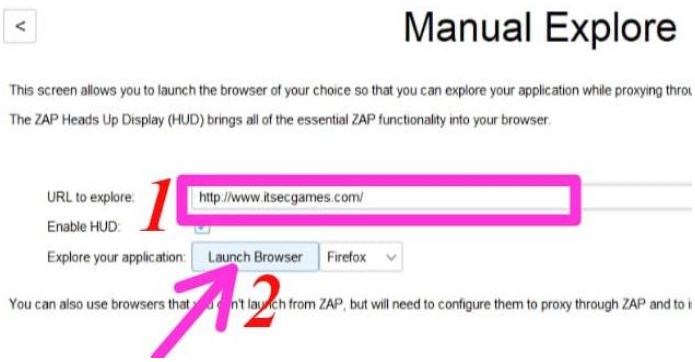



- Step 9: - Now click on Alerts section and analyze type of risk which was exposed by automated scan



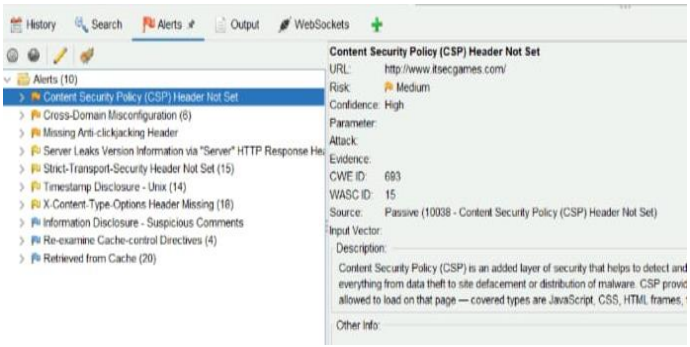
***Manual explore:**

- Step 1: - Open the OWASP ZAP & click on manual explore to manually scanning website and paste BW app URL. Then click on launch browser



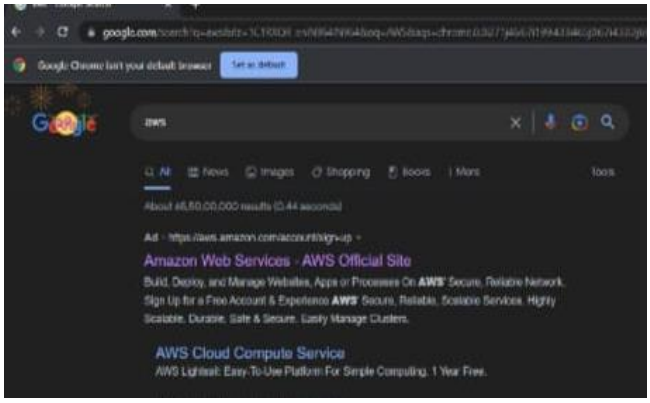

- Step 2: - Which opens BW app website.


- Step 3: - From website we can start spider and manual scanning. Now come Back to ZAP and check for alerts.



**13) Create a cloud account in AWS & Access the IAM user service & create two user accounts & one group and add 2 created users to the group and setup two factor authentication to any one user.**

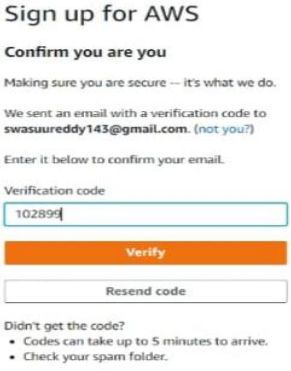
- **Step 1: -** Open the chrome browser & search the AWS then click on the amazon web services-AWS official site




- **Step 2: -** Then click on create a free account

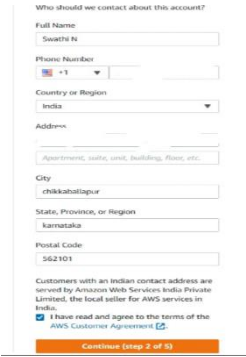

- **Step 3: -** Enter your email address & AWS account name then click on verify email address


- **Step 4: -** Enter verification code then click on verify

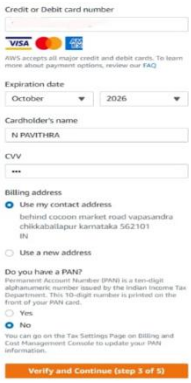


- **Step 5: -** Enter Root user password & confirm the password then click on Continue

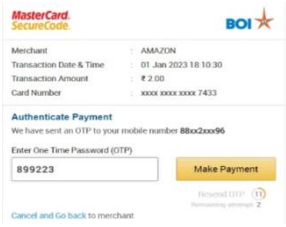

- **Step 6: -** Full fill the contact information then click on continue




- **Step 7: -** Full fill the billing information then click on verify and continue



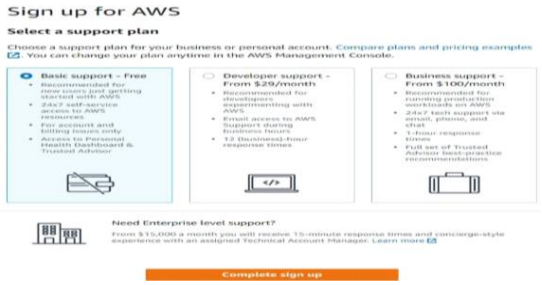

- **Step 8: -** Enter one time password (OTP) then click on make payment




- **Step 9: -** Enter your phone number & captcha then click on send SMS

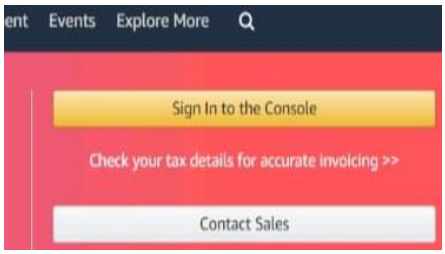
- Step 10: - Then enter the verification code


- Step 11: - Then click on complete sign up



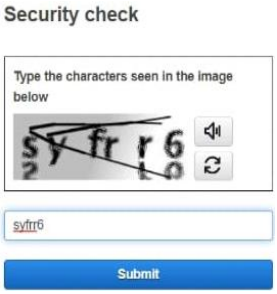

- Step 12: - Click on Go to AWS management console


- Step 13: - Click on sign in to the console



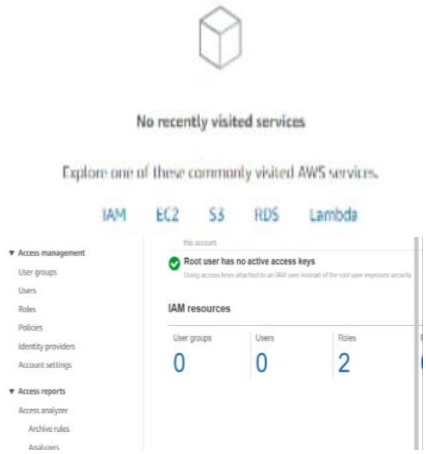

- Step 14: - Select the IAM user & enter your email address then click on Next


- Step 15: - Enter the captcha then click on submit

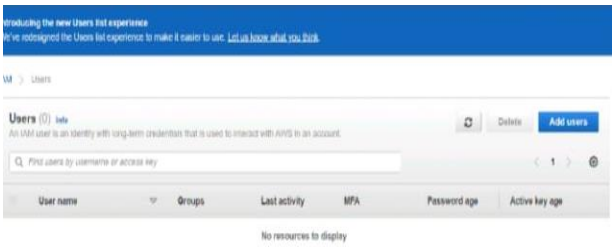


- Step 16: - Enter your password then click on sign in option


- Step 17: - Then click on IAM
- Step 18: - Click on user



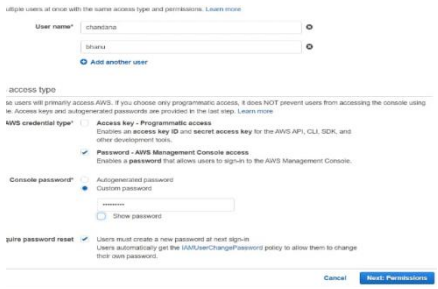

- Step 19: - Then click on Add user



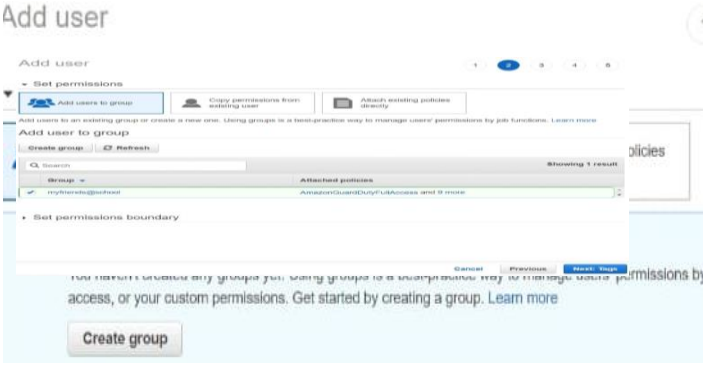

- Step 20: - Enter user name then if you want add multiple user

  Choose Add another user for each additional user & type their user names

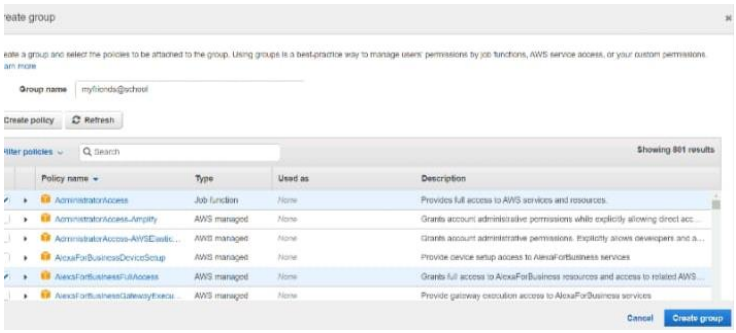
  Select the password – AWS MCA. then Select the customer password & Enter the password. Then click on Next: permission



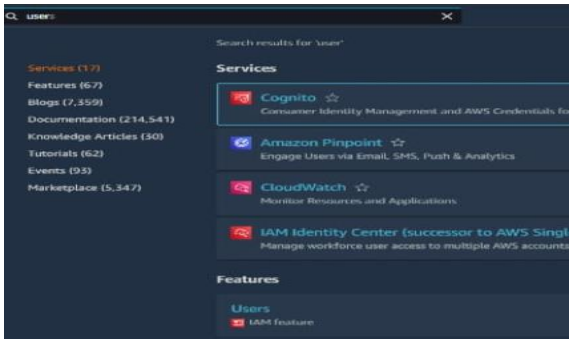
- Step 21: - Click on create group




- Step 22: - Enter the group name & Give a policies then click on create group



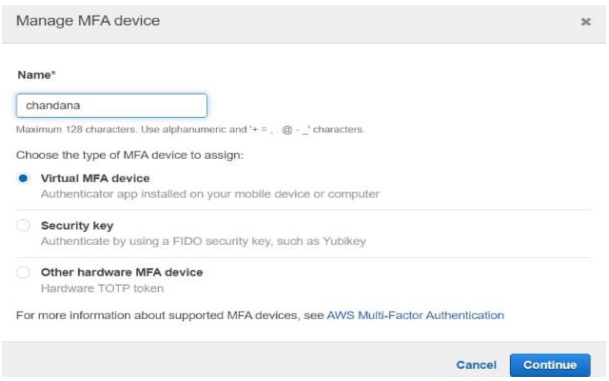

- Step 23: - Then group will be created
- Step 24: - Search the users then click on users




- Step 25: - Then click on Add MFA


- Step 26: - Then click on Activate MFA

- Step 27: - Enter the user name then click on continue




- Step 28:-Then download the google authentication app in your phone
- Step 29:-Then scan the QR code to add your AWS account to the

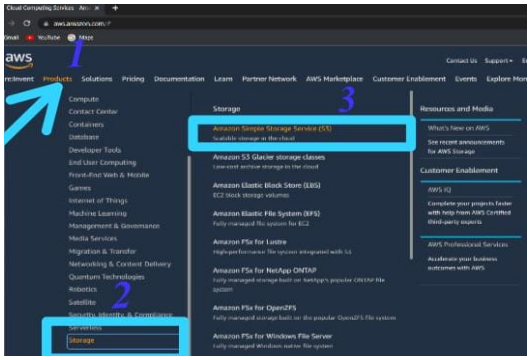
  Authenticator app


- Step 30: - Enter the numeric code from the authentication into the AWS console. Then wait for a new code to appear in the authenticator.

  Enter the second code. Then click on “Assign MFA”

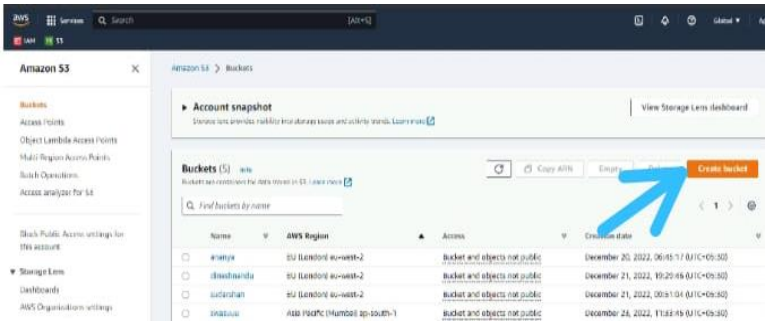
**14) Demonstrate the creation of S3 bucket service in AWS & store some files in S3 bucket.**

- Step 1: - After login, go to products in AWS & select the storage option then click on the Amazon simple storage service(S3)

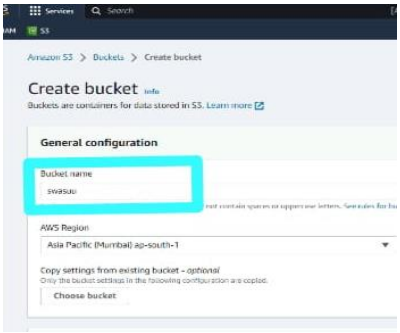



- Step 2: - Click on Get started with amazon S3

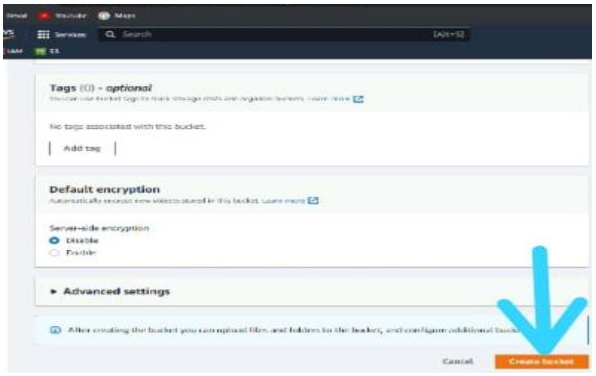

- Step 3: - Then click on create bucket



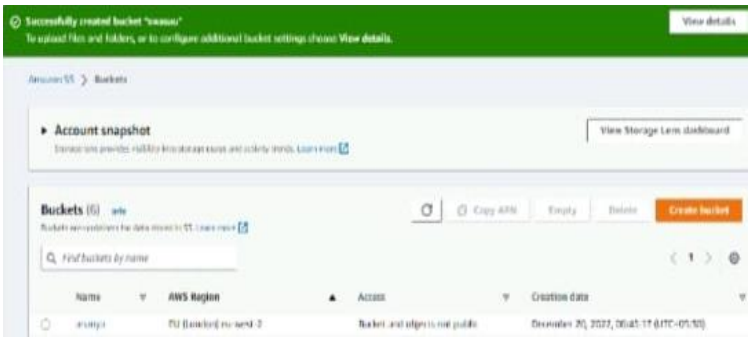

- Step 4: - Enter the bucket name then scroll down



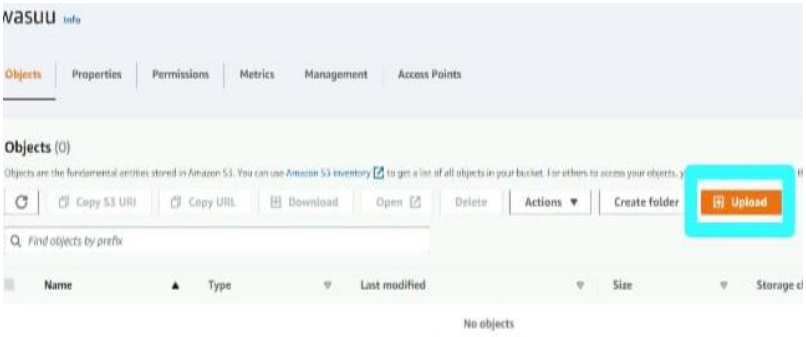
- Step 5: - Click on create bucket



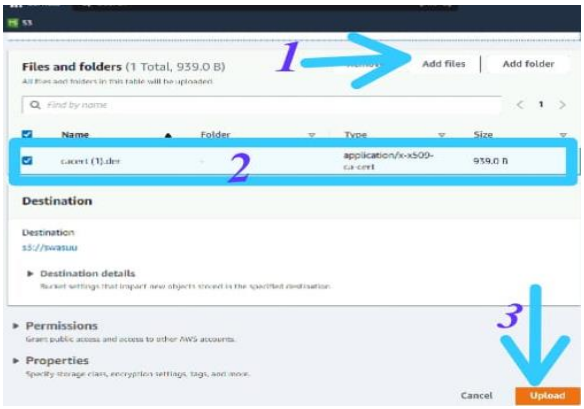

- Step 6: - Then bucket will be created



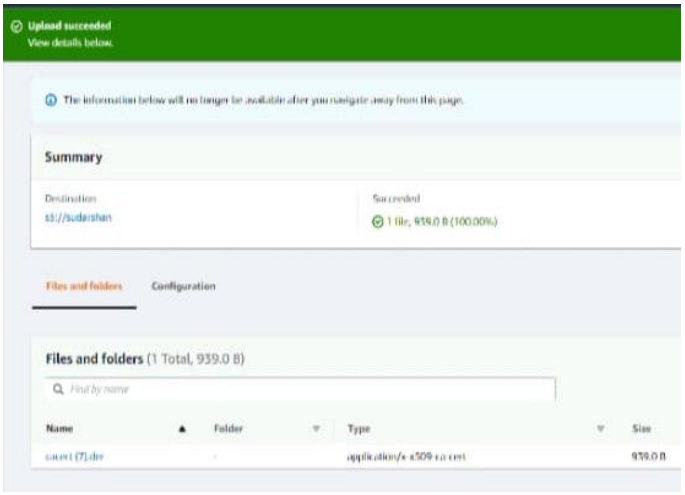

- Step 7: - Select the bucket then click on the upload option




- Step 8: - Click on the Add files then click on the upload

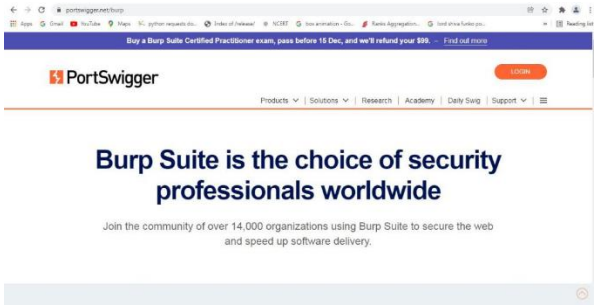


- Step 9:- Then file will be uploading to S3 bucket.

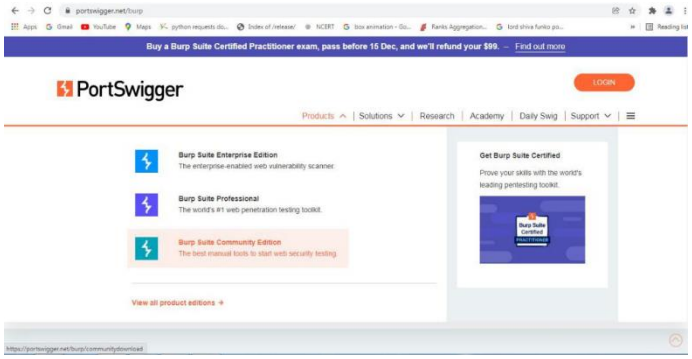


## 15) Installing Burp Suite on Windows & Import proxy server CA certificate to browser

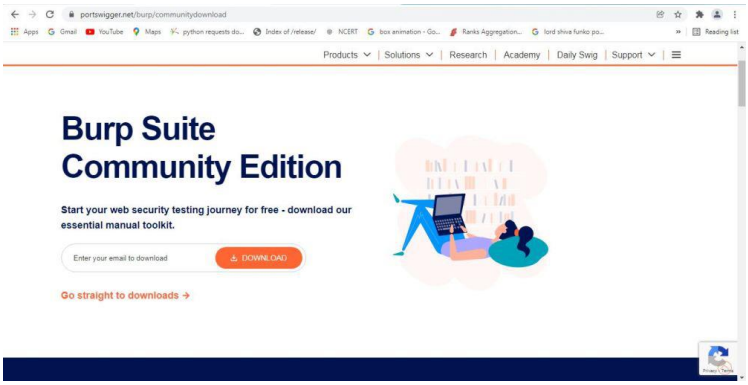
- **Step 1:** Visit the official Burp Suite website using any web browser.



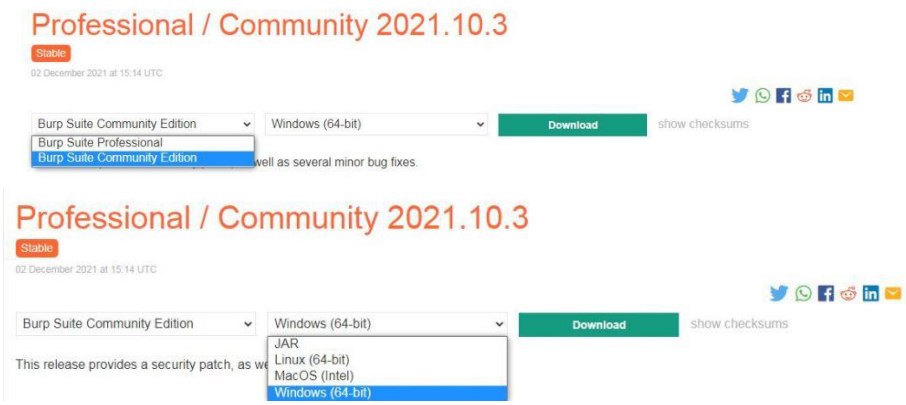

- **Step 2:** Click on Products, a list of different Burp Suites will open, choose Burp suite Community Edition as it is free, click on it.



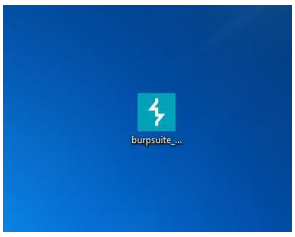

- **Step 3:** Click on Go straight to downloads.



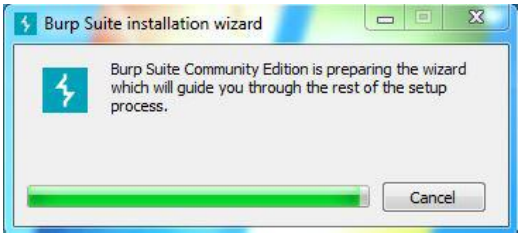

- **Step 4:** select Burp suite community edition and select windows (64-bit) and then click on download.



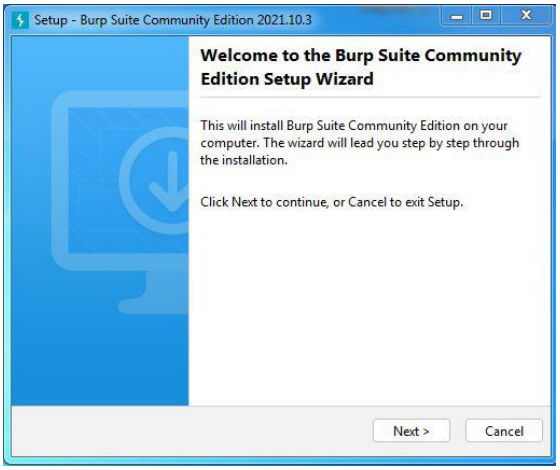
- **Step 5:** Now check for the executable file in downloads in your system and run it.



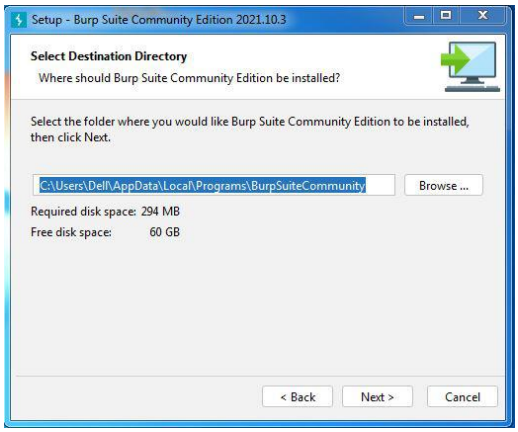

- **Step 7:** Loading of Installation Wizard will appear which will take a few seconds.



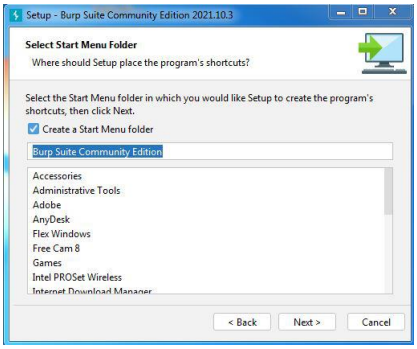

- **Step 8:** click on Next.



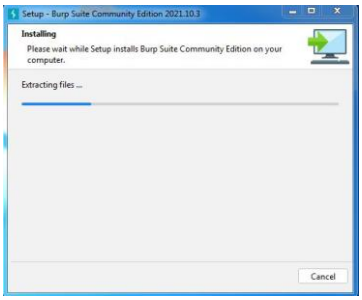

- **Step 9:** choose the drive which will have sufficient memory space for installation. It needed a memory space of 294 MB.



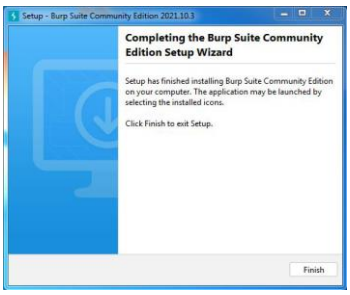
- **Step10:** click on Next Button.



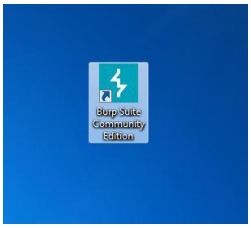

- **Step 11:** installation process will start and will hardly take a minute to complete the installation.



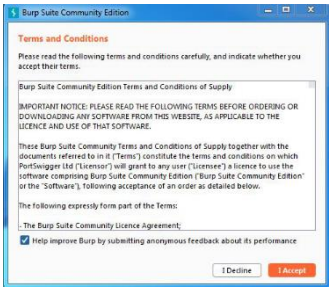

- **Step 12:** Click on Finish



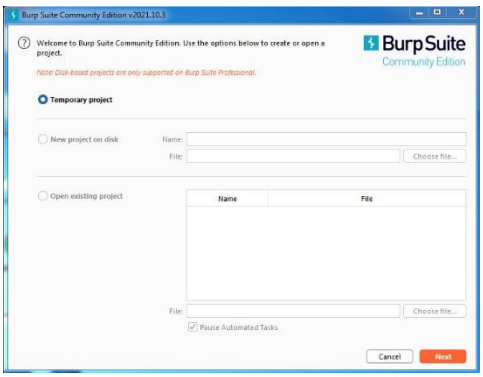

**Step 13:** Burp suite is successfully installed on the system and an icon is created on the desktop



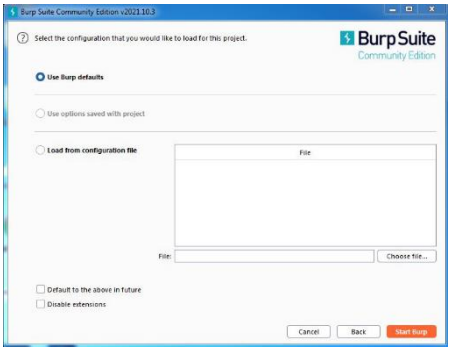

**Step 14:** Run the software, Click on I Accept.



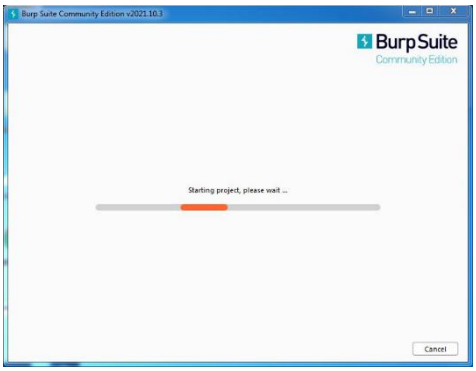
- **Step 15:** Choose click Next.



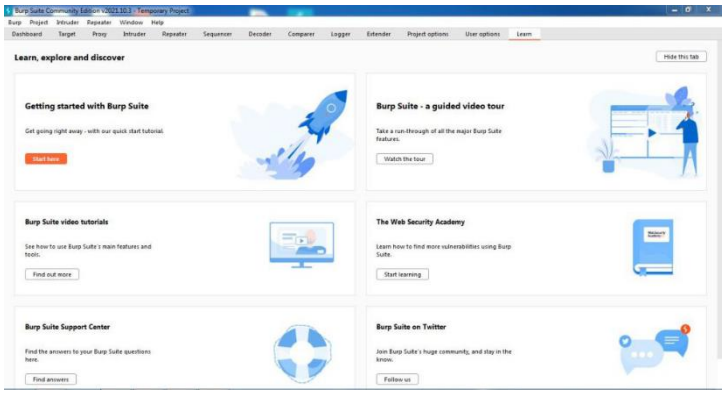

- **Step 16:** click on Use Burp Defaults.




- **Step 17:** Project will start loading.

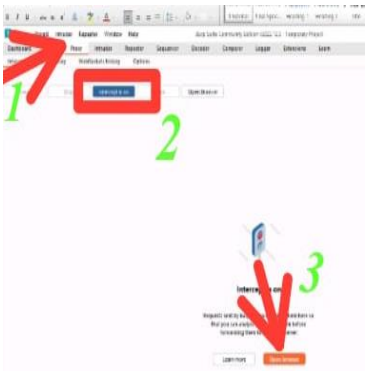



- **Step 18:** Finally new project window will appear.



❖ **Certificate import to browser**

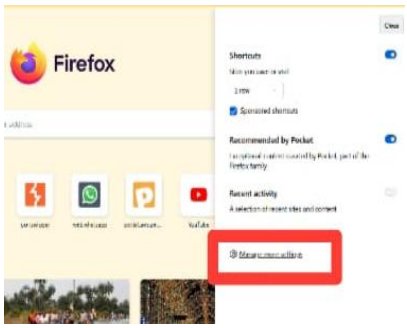
- Step 1: - Double click on the burp suite app & click on the next then click on the Start burp
- Step 2: - Now burp suite will be open & select the proxy and turn on the Intercept then click on the open browser option



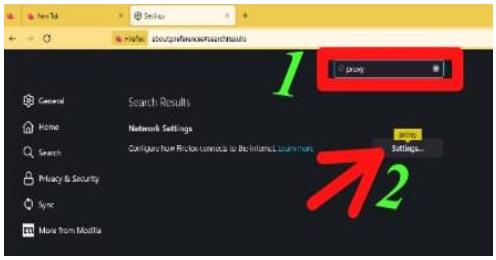

- Step 4: - Search the http://Burpsuite then click on the CA certificate
- Step 5: - Then CA certificate will be downloaded


- Step 6: - Open the fire fox then go to settings


- Step 7: - Then click on the manage more settings

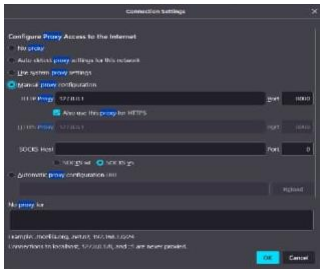


- Step 8: - Search the proxy then click on the proxy settings

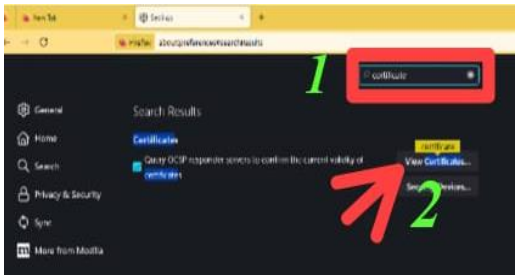



- Step 9: - Choose the manual proxy configuration & enter the HTTP proxy and

  Port then click on ok option EX: - 127.0.0.1 & 8080

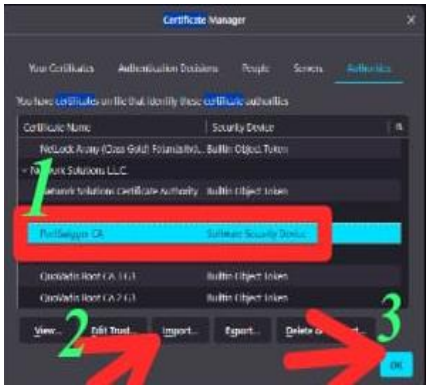


- Step 10: - Search the certificate then click on the view certificates




- Step 11: - Select the port swigger CA certificate & Import the certificate then

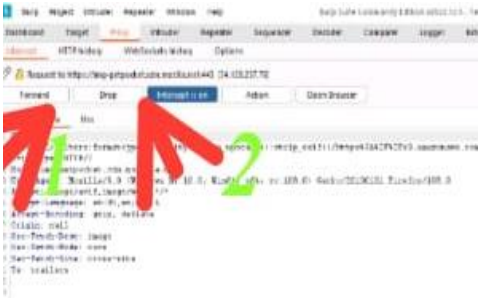
  Click on the ok option



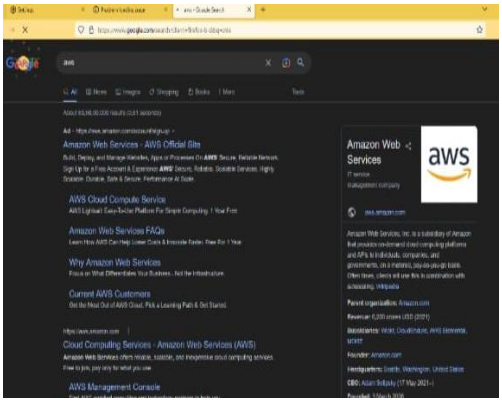

- Step 12: - Open the fire fox then search the any website name\

- Step 13: - Now we can't reach the website, So

- Step 14: - Open the burp suite & click on the forward option then click on drop



- Step 15**: -** Now we can reach the website



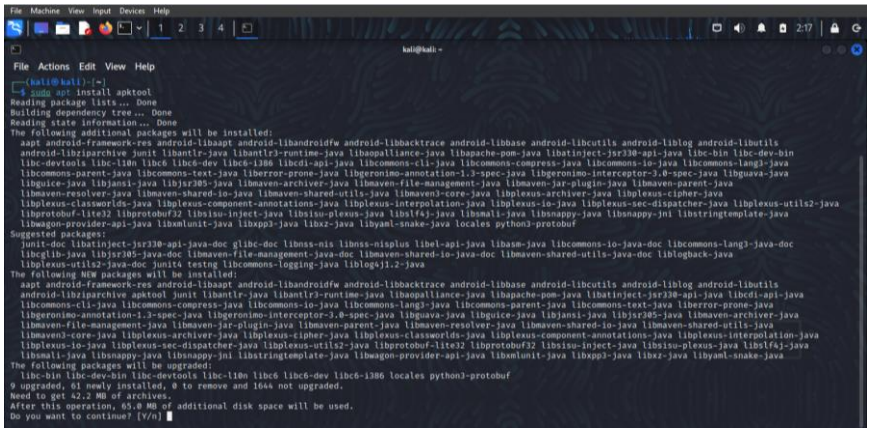
**16) Install the Apktool on your Virtual machine and perform reverse engineering on the DIVA Android application.**

- Step 1:- Open terminal in kali linux

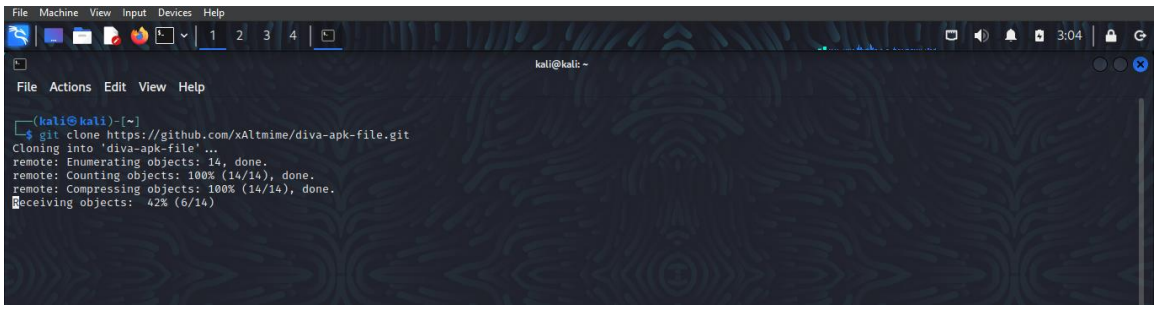

- Step 2 :- Install apktool using this command **"sudo apt install apktool"** & press Enter button


- If installation not begin / any error show update **"sudo apt update"**

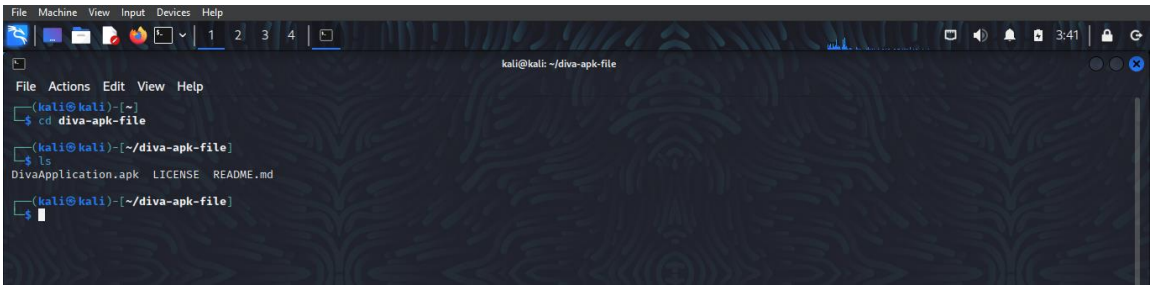

- Step 3:- Wait untill installation complete



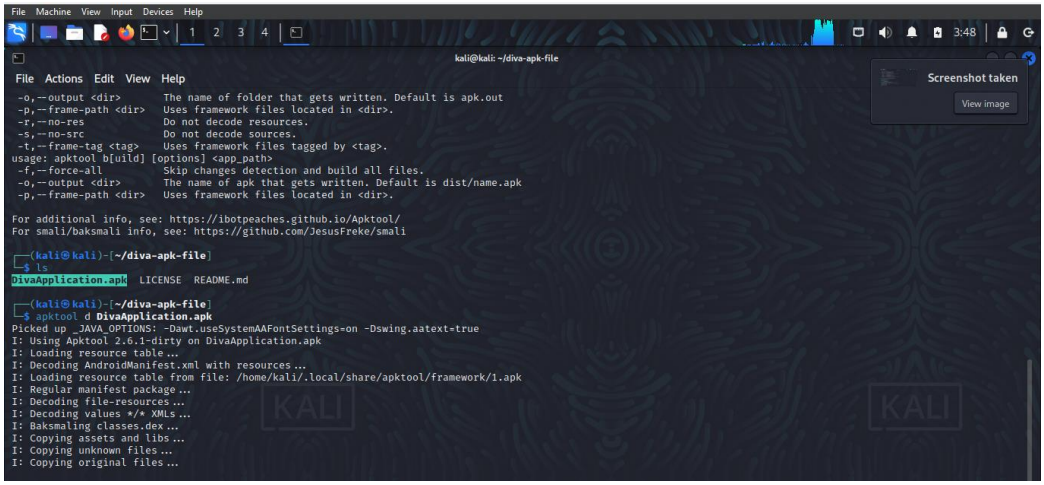

- Step 4:- Download Diva application using **"git clone https://github.com/xAltmime/diva-apk-file.git**



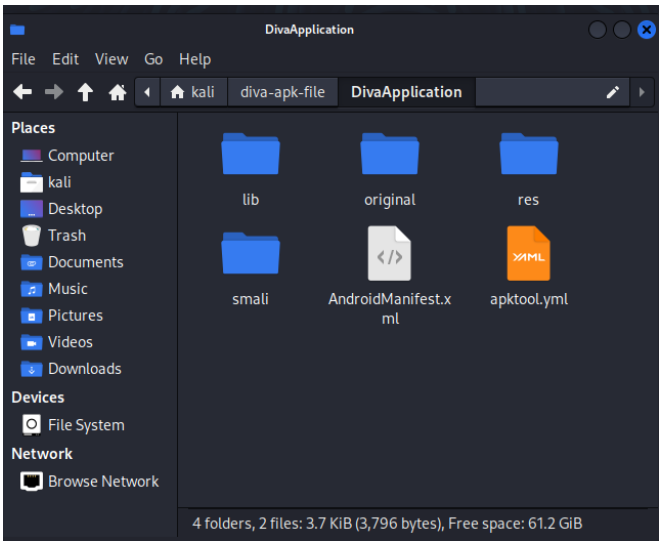
- Step 5:- Now change directory to **“diva-apk-file”** using **“cd diva-apk-file”**




- Step 6:- Now decoding the **“DivaApplication.apk”** using **“apktool d DivaApplication.apk”**

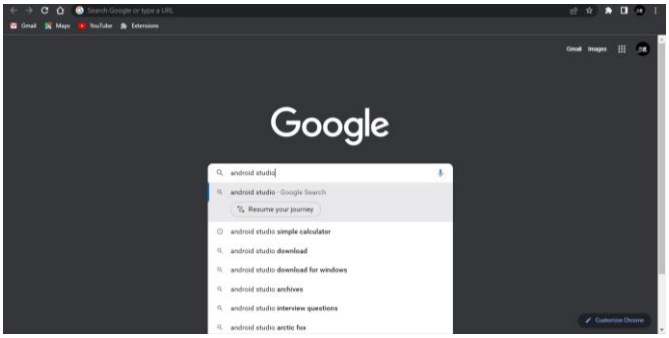



- Step 7 :- After decoding complete go to **“DivaApplication”** Folder thare you can see the application source code

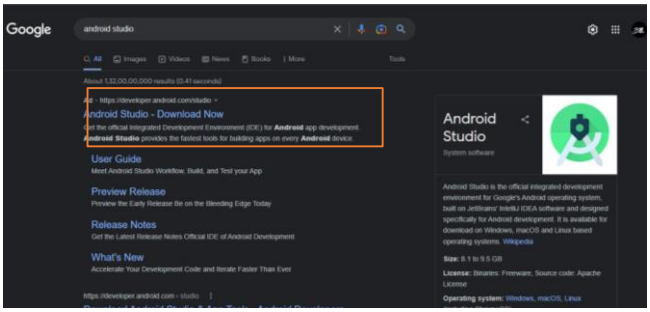


## 17) Download and install the android studio and create a AVD

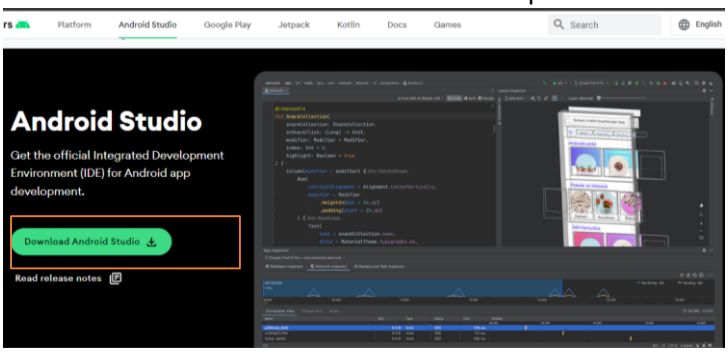
- Step 1:- go to google and search android studio




- Step 2:- Click on Android Studio – download now option

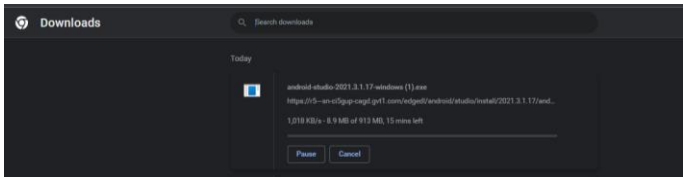



- Step 3:-Now click downlod android studio option & and click terms and conditions and press Download android studio Dolphin

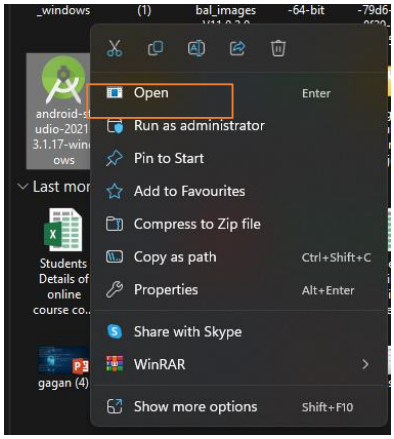




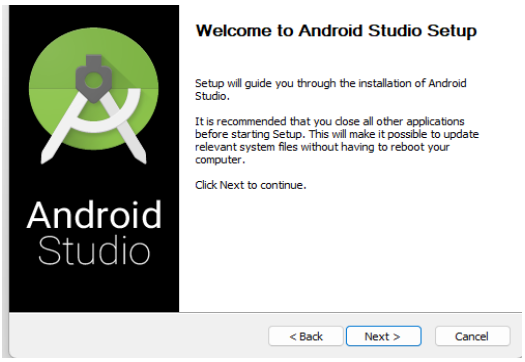
- Step 4:- Wait untill download complet

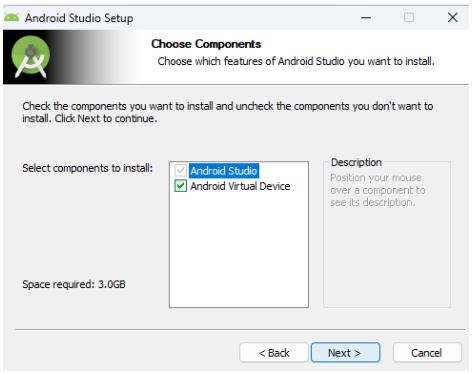



- Step 5:- After complet the download open the software

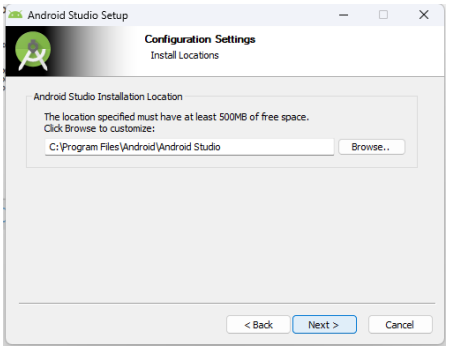


- Step 6:- Click next button and Choose Components and click next.

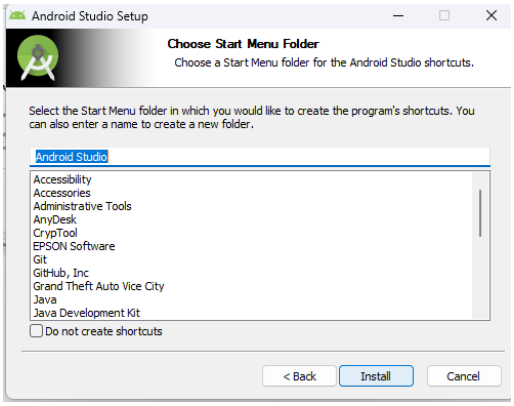


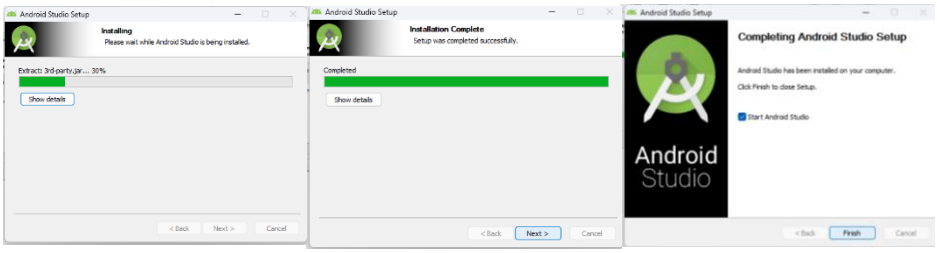

- Step 7:- Select File save location and click next.



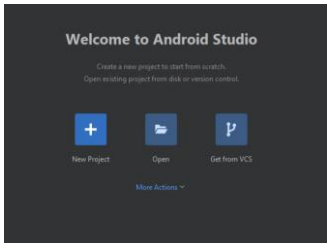

- Step 8:- select Installation Directory's and click install



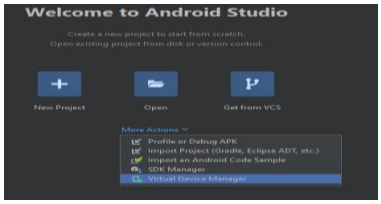

- Step 9:- Wait untill installation complete now click next and finish button



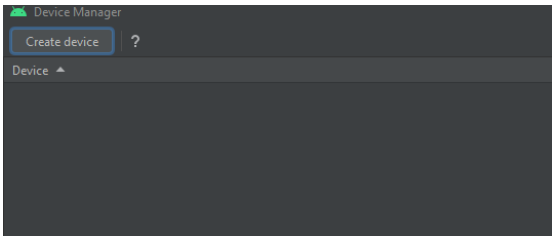

- Step 10:- Click on more Actions



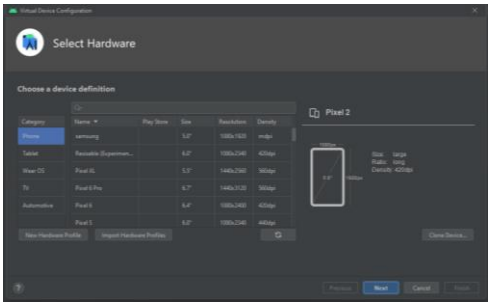
- Step 11:- Now click on Virtual Device Manager



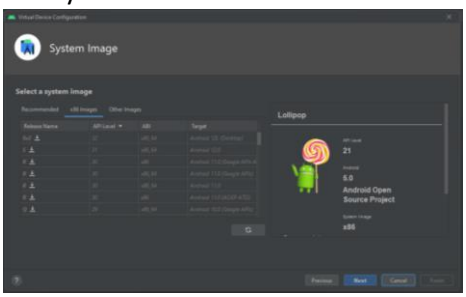

- Step 12:- Click on create device



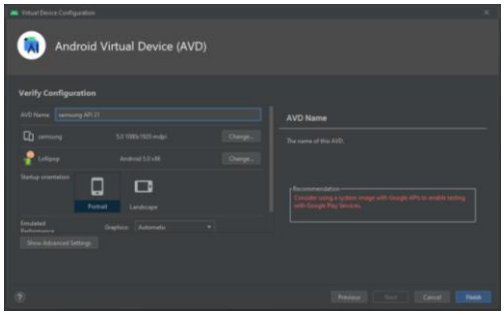

- Step 13:-select any one category & model then click next



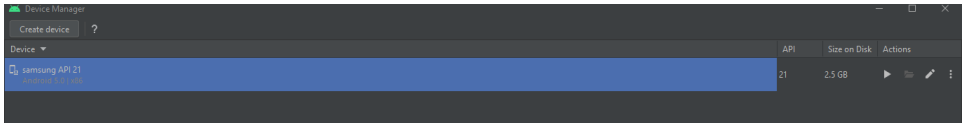

- Step 14:- select any one android version and click next




- Step 15:- type a AVD name and click finish



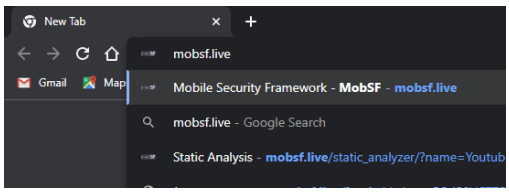

- Step 16:- AVD device created



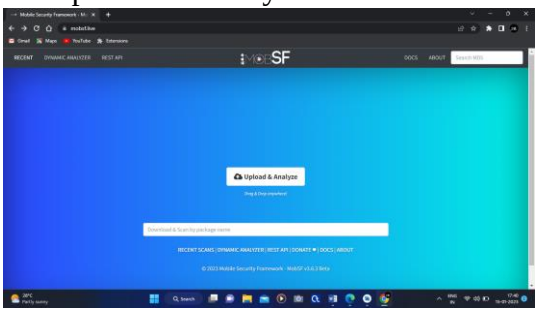
## 18) Scan any 5 android apps and analyse the report's using MobSF

- Step 1:- go to any one browser and download any 5 android apps like **"youtube go, Instagram lite,fb lite, snaptube,dr driving"**

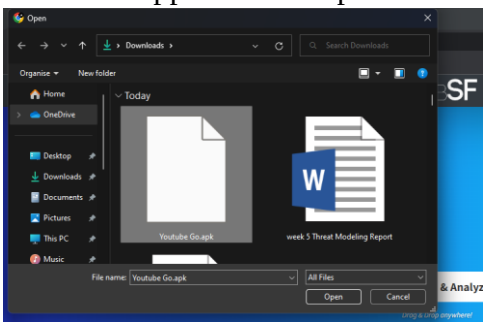

- Step 2:- after download the apps open any browser and search **"mobSf.live"**



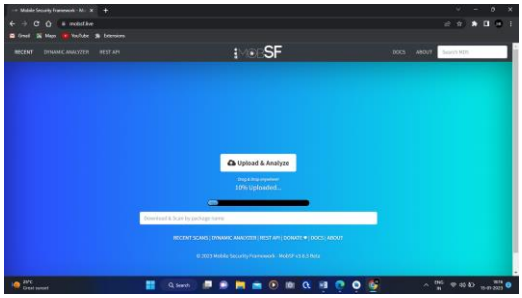

- Step 3:- Then click on upload and analyse



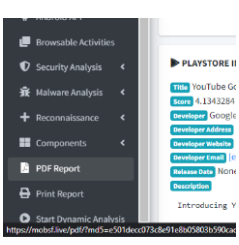

- Step 4:- Select any one android app and click open

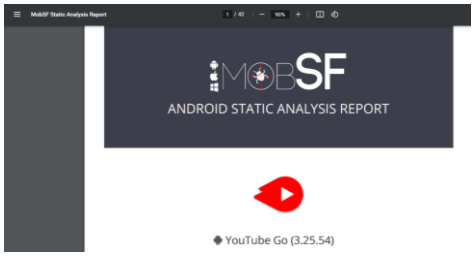



- Step 5:- wait until complet the upload and analyse




- Step 6:- after complet the analyse click on pdf report and save the report and analyse the report

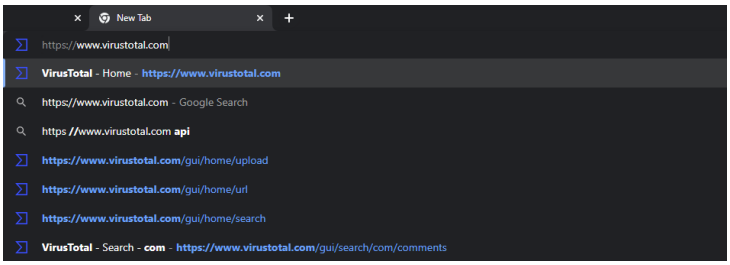



- Step 7:- repeat the same steps for all apps

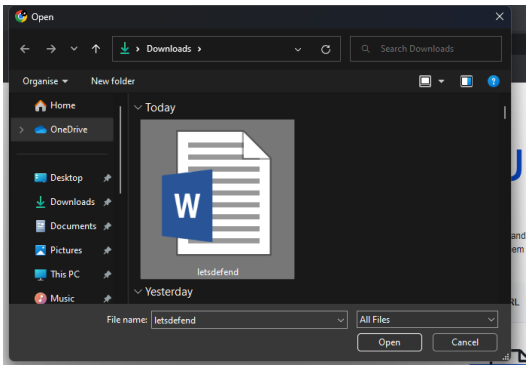
## 19) Using VIRUSTOTAL website Analyse any File, Url & Domain etc…

- Step 1:- Go to any browser and search https://www.virustotal.com




- Step 2:-Click choose file to scan a file


- Step 3:- Select any file and click open

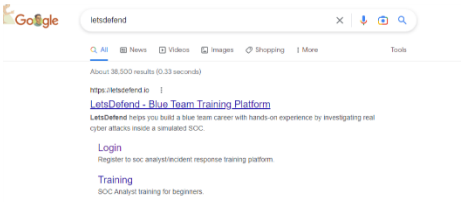



- Step 4:-Now select URL option and enter any url and click enter to start a scan

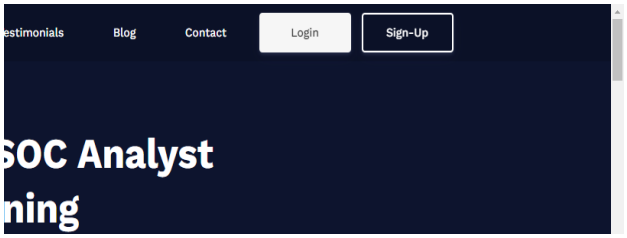

- Step 5:-Now select search and enter URL, Domain,, IP address and press enter

**20) Give the procedure for Understanding the tools and products used in any organisation using letsdefend.io website**

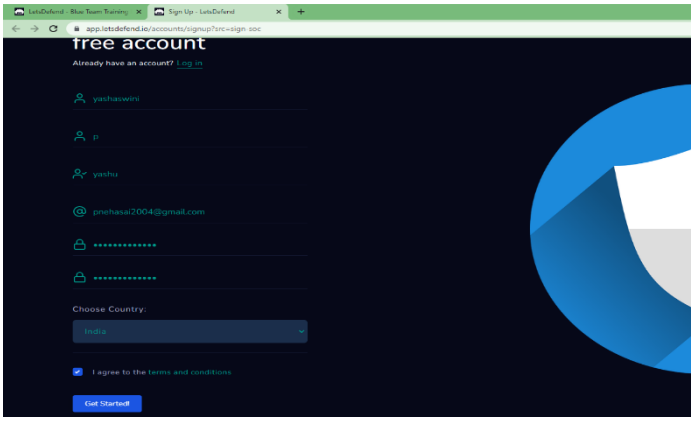
- **Step 1:** open google chrome and search for letsdefend



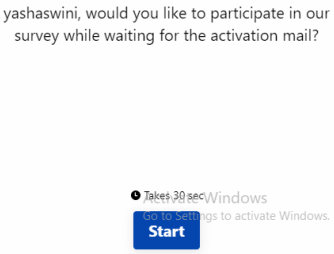

- **Step 2:** Click on Sign-Up



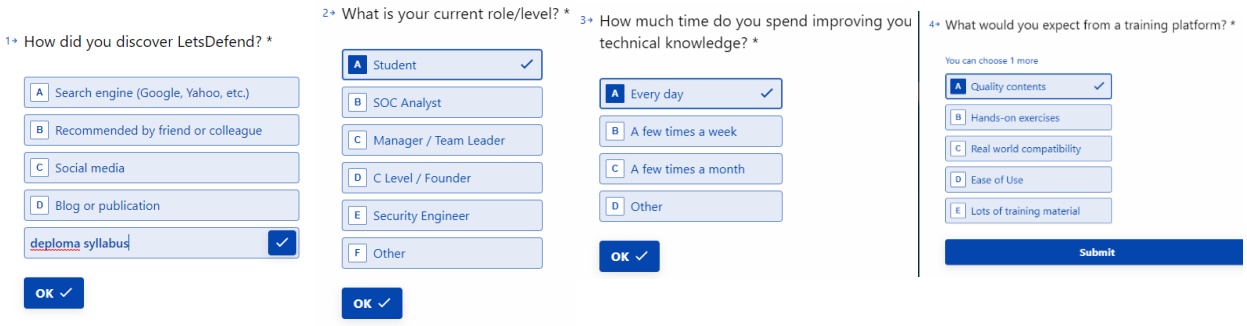

- **Step 3:** give a details for the log in and Click on Get Started



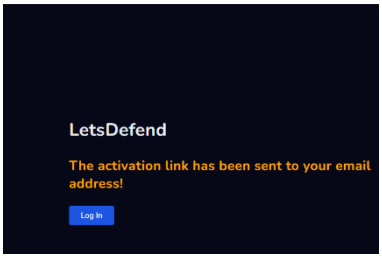

- **Step 4:** Click on Start



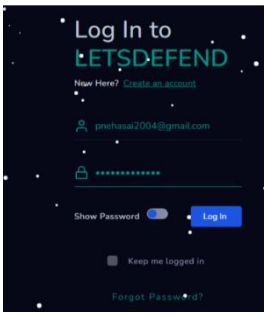

- **Step 5:** choose an answers for the given questions



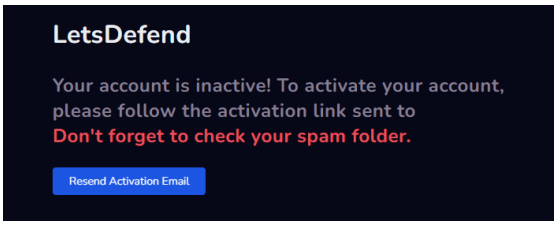
- **Step 6**: Click on log in

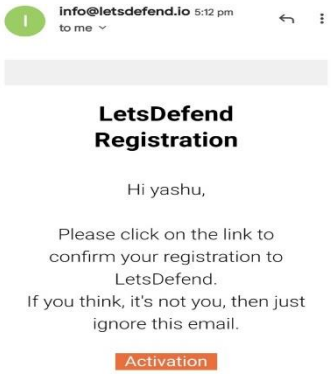



- **Step 7**: give an email and password for log in

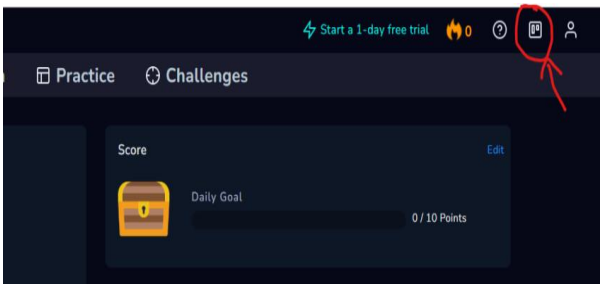



- **Step 8:** go to gmail in your mobile for activation and Click on Activation

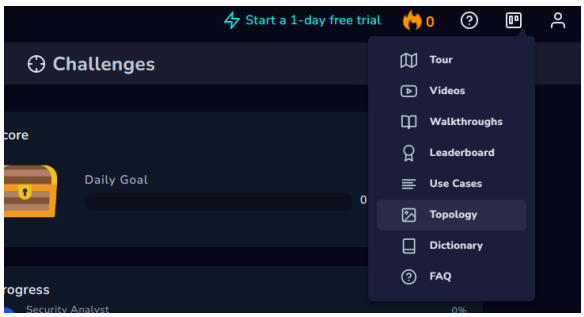



- **Step 9:** Click on the Square Box




- **Step 10:** Click on Topology



- **Step 11:** The chart or the diagram will be displayed on the screen