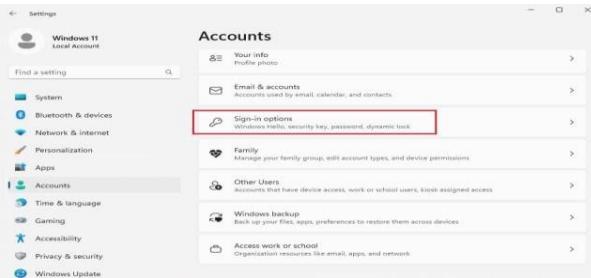


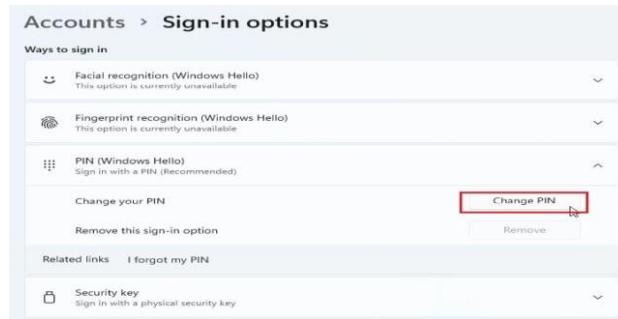
1) Change/set windows desktop security pin/ password & check windows update system

❖ Password setup or change pin

- Step1:- press the windows 11 keyboard shortcut “windows + l” 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**

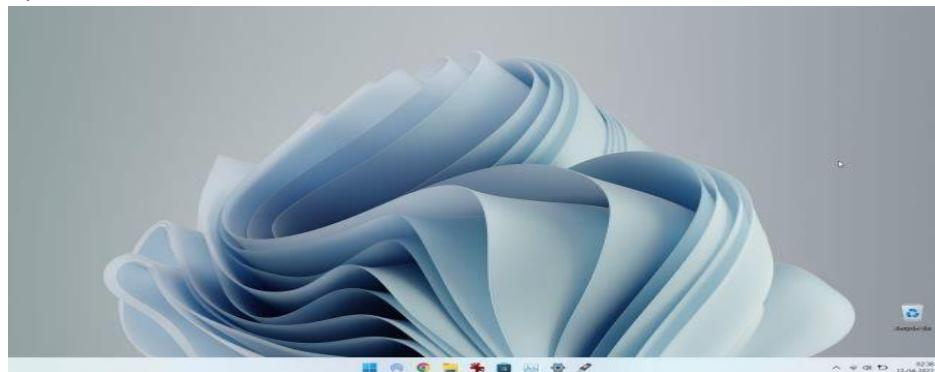
- Step1:- first press the windows 11 keyboard shortcut “windows + I” to open the settings app. Next, navigate to the “windows update” section from the left sidebar.



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

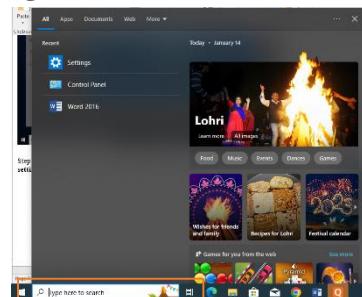


- Step3 :-after that the update will be installed, and you will be asked to restart your pc. Simply reboot Your windows 11 pc in no time.

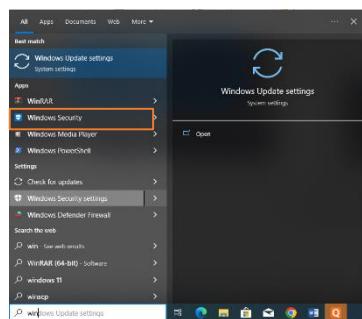


2) Demonstrate Turn on & off Windows OS Firewall

➤ Step 1: go to search



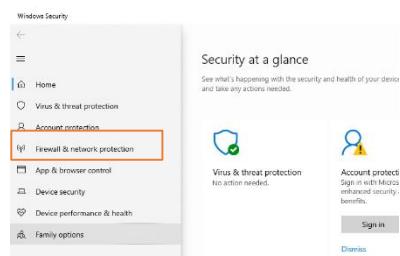
➤ Step 2: search windows security



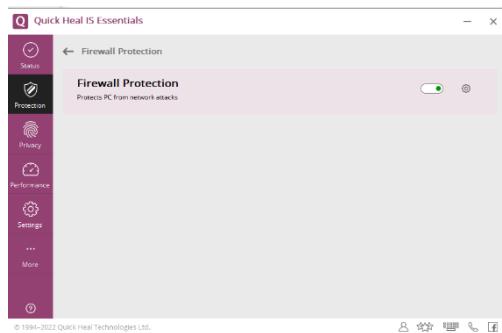
➤ Step 3: Click on Navigation button



➤ Step 4: Click on Firewall and network protection



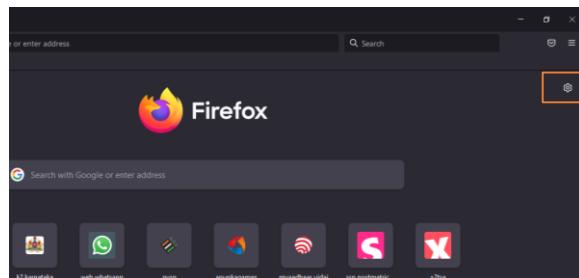
➤ Step 5 :- if you installed any anti-virus software's the firewall will open in app , now you can on & the firewall



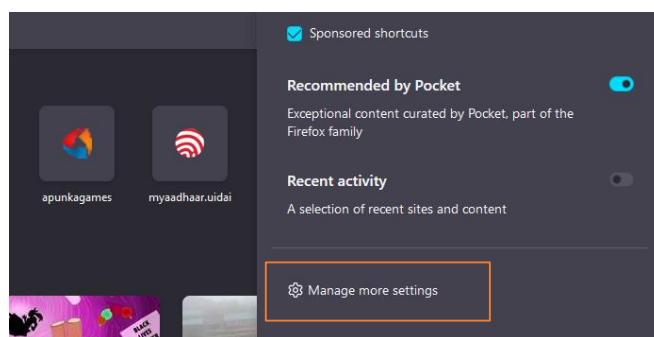
3) Check the browser and website certificates and analyze the certificates

❖ Browser certificates view

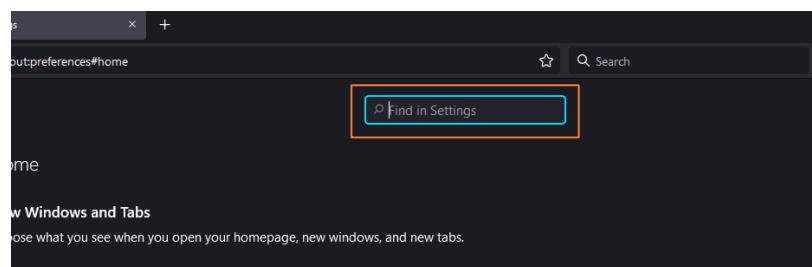
- Step 1:- Open Firefox Browser and click on settings icon



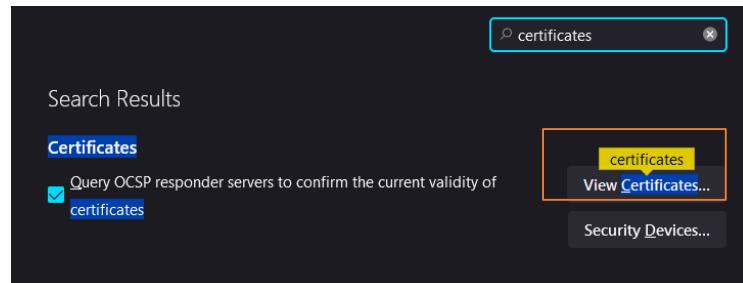
- Step 2:- click manage more setting option



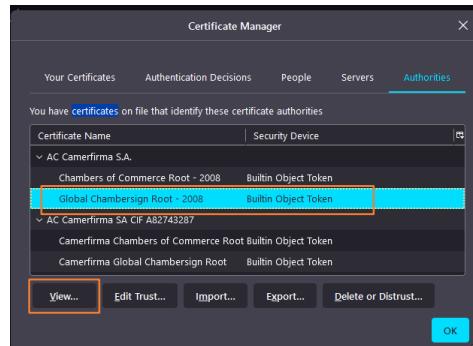
- Step 3:- Search certificates in search box



- Step 4:- Click on view certificates



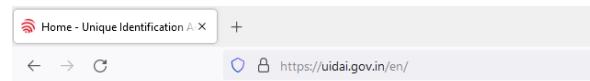
- Step 5:- Select any one certificate and click view



- Step 6:- Now you can see the certificate

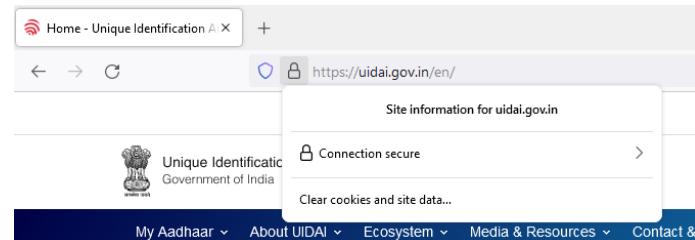
❖ Website certificate check

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

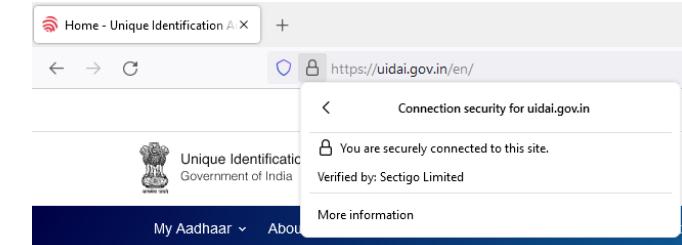


My Aadhaar ▾ About UIDAI ▾ Ecosystem ▾ Media & Resources ▾ Contact &

- Step 3:-Click connection secure



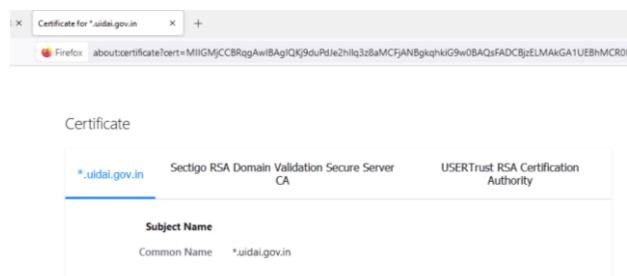
- Step 4:- Click more information



- Step 5 :- Now click view certificate



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

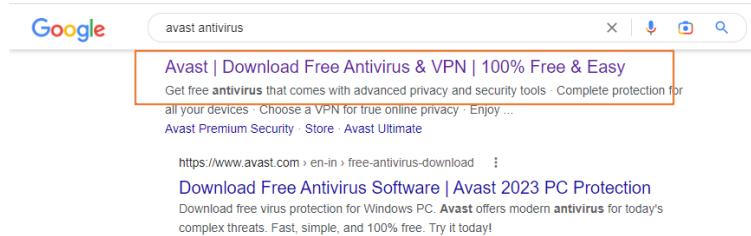


4) Install Anti-virus and scan the computer.

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



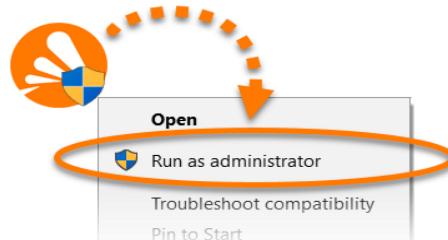
- Step 2:- click on avast download free antivirus & vpn link



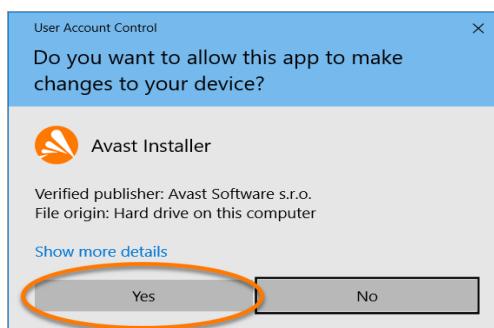
- Step 3:- click on Download free protection button



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



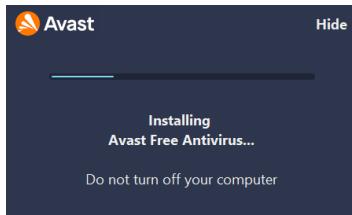
- Step 5: If prompted for permission by the User Account Control dialog, click Yes.



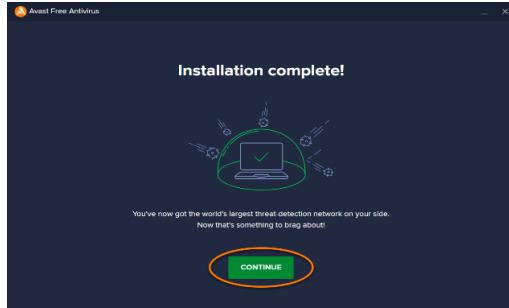
- Step 6: Then, click Install



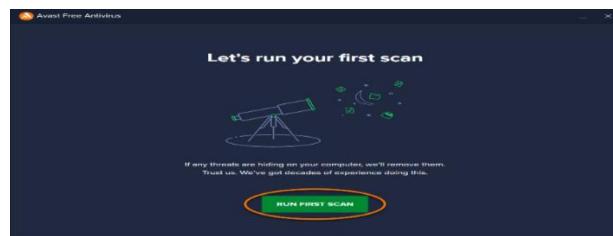
- Step 7: Wait while setup installs Avast Free Antivirus on your PC.



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



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



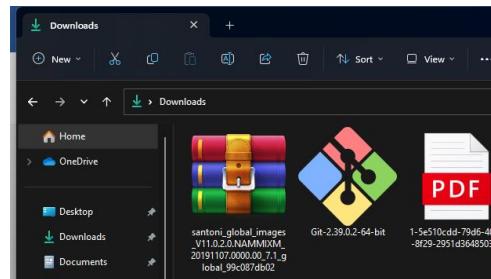
5) Install Git app and perform the basic git operations below

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

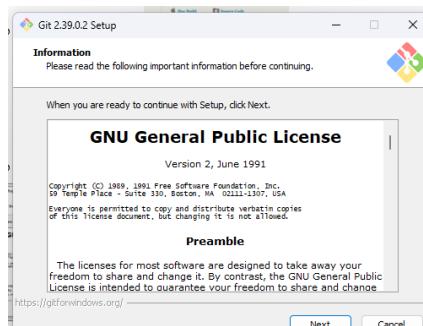
- Step 1: Browse to the official Git website: <https://git-scm.com/downloads>
- Step 2: Click the download link for Windows and allow the download to complete.



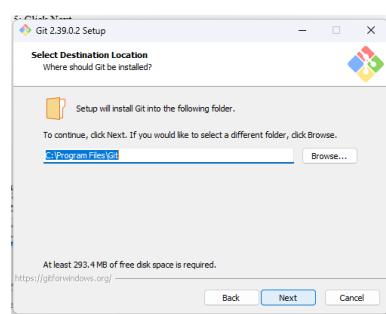
- Step 3: Double-click the file to extract and launch the installer.



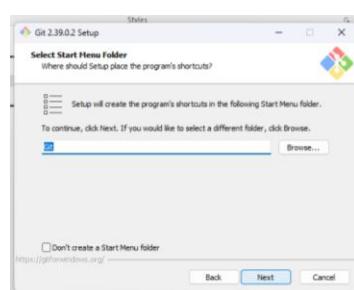
- Step 4: Click Next.



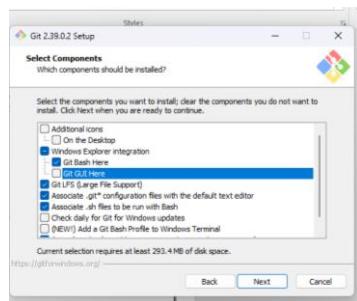
- Step 5: Click Next.



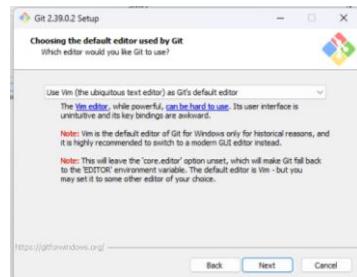
- Step 6: Click Next.



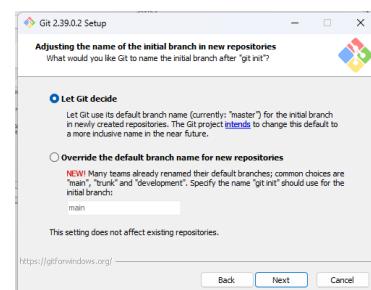
➤ Step 7: Simply click Next.



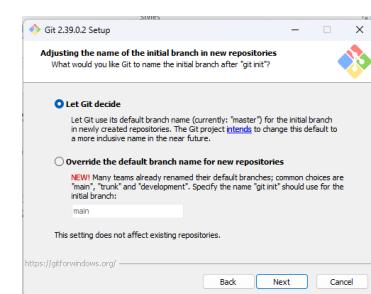
➤ Step 8: Click Next.



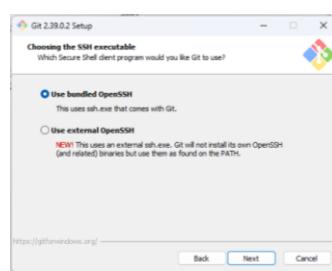
➤ Step 9: Click Next.



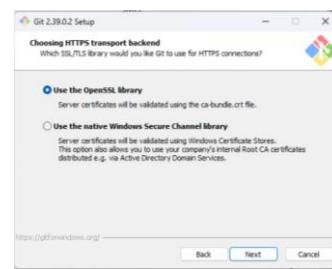
➤ Step 10: Click Next.



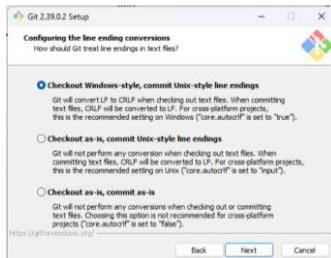
➤ Step 11: Click Next.



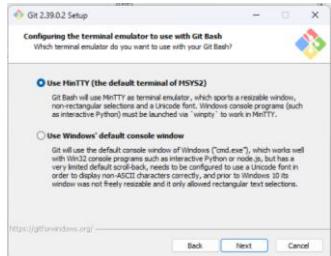
➤ Step 12: Click Next.



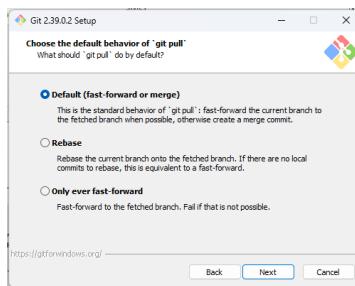
➤ Step 13: Click Next.



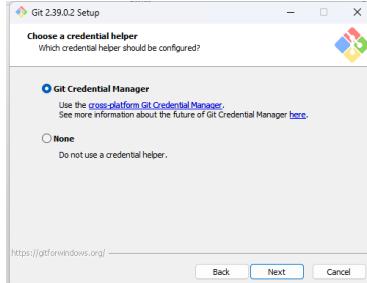
➤ Step 14: Click Next.



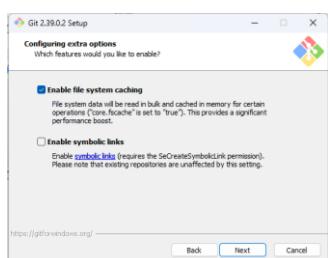
➤ Step 15: Click Next to continue with the installation.



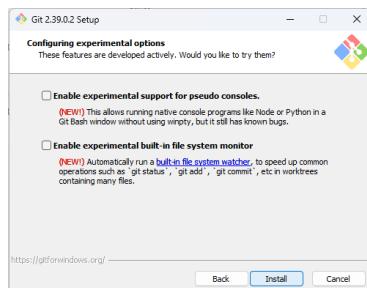
➤ Step 16: Click Next.



➤ Step 17: Click Next.



➤ Step 18: Click Install.



- Step 19: Click Finish.



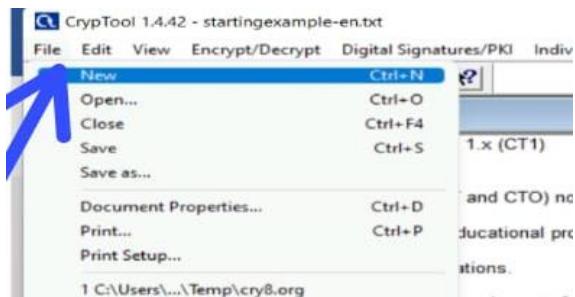
basic git operation

- 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,

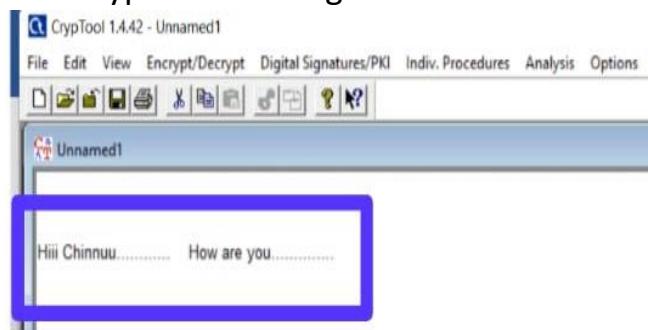
6) Design a simple crypto system [encryption, decryption, digital signature] using any crypto tool

❖ Steps for Encryption

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



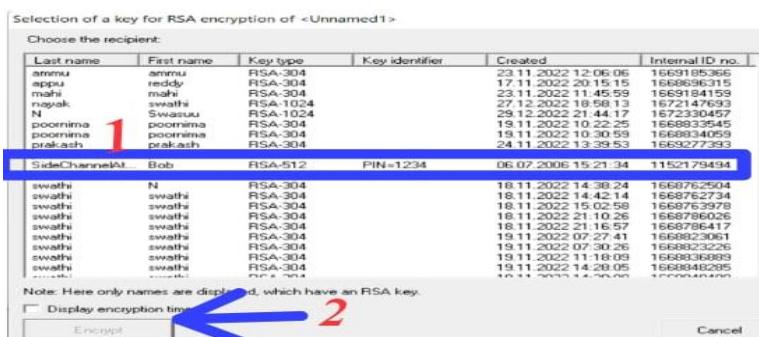
➤ Step 2: - Then type the message



➤ 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



❖ Steps for Decryption

- 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

| Select your secret key from the PSE list. | | | | | |
|---|------------|----------|----------------|---------------------|----------------|
| list name | First name | Key type | Key identifier | Created | Internal ID no |
| rathin | ammu | RSA-304 | | 23.11.2022 12:06:06 | 16689185366 |
| ipu | reddy | RSA-304 | | 17.11.2022 20:15:15 | 16689696315 |
| shi | mahi | RSA-304 | | 23.11.2022 11:45:59 | 1669184159 |
| gopal | sudu | RSA-304 | | 27.11.2022 14:40:24 | 16689766039 |
| poornima | Swasuri | RSA-1024 | | 29.12.2022 21:44:17 | 1672330457 |
| poornima | poornima | RSA-304 | | 19.11.2022 10:22:25 | 1668833545 |
| poornima | poornima | RSA-304 | | 19.11.2022 10:30:59 | 1668834059 |
| prakash | prakash | RSA-304 | | 24.11.2022 13:39:53 | 1669277393 |
| SideChannelAttack | Bob | RSA-512 | PIN=1234 | 06.07.2006 15:21:34 | 1152179494 |
| rathi | N | RSA-304 | | 18.11.2022 14:38:24 | 1668762504 |
| rathi | swathi | RSA-304 | | 18.11.2022 14:42:14 | 1668762734 |
| rathi | swathi | RSA-304 | | 18.11.2022 15:02:58 | 1668762778 |
| rathi | swathi | RSA-304 | | 18.11.2022 15:03:09 | 1668766039 |
| rathi | swathi | RSA-304 | | 18.11.2022 21:16:57 | 1668768417 |
| rathi | swathi | RSA-304 | | 19.11.2022 07:27:41 | 1668823061 |
| rathi | swathi | RSA-304 | | 19.11.2022 07:30:26 | 1668823226 |
| rathi | swathi | RSA-304 | | 19.11.2022 11:18:09 | 1668976389 |

Note: Only PSEs containing an RSA key are shown.
Display decryption time

Decrypt Cancel

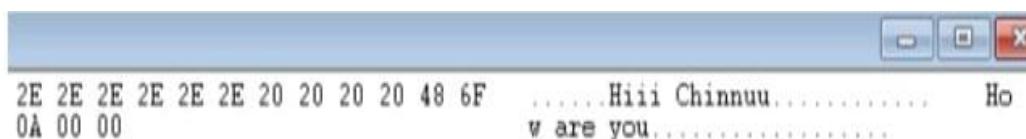
- Step 4: - Enter the PIN code Then click on the Decrypted

| Note: Only PSEs containing an RSA key are shown. | | | | | |
|--|----------|---------|----------|---------------------|------------|
| Display decryption time | | | | | |
| poornima | poornima | RSA-304 | | 19.11.2022 10:22:25 | 1668833545 |
| poornima | poornima | RSA-304 | | 19.11.2022 10:30:59 | 1668834059 |
| prakash | prakash | RSA-304 | | 24.11.2022 13:39:53 | 1669277393 |
| prakash | prakash | RSA-304 | | 24.11.2022 14:00:26 | 1669278626 |
| SideChannelAttack | Bob | RSA-512 | PIN=1234 | 06.07.2006 15:21:34 | 1152179494 |
| sudu | sudu | RSA-304 | | 19.11.2022 10:24:26 | 1668833666 |
| rathi | N | RSA-304 | | 18.11.2022 14:38:24 | 1668762504 |
| rathi | swathi | RSA-304 | | 18.11.2022 14:42:14 | 1668762734 |
| rathi | swathi | RSA-304 | | 18.11.2022 15:02:58 | 1668763978 |
| rathi | swathi | RSA-304 | | 18.11.2022 21:10:26 | 1668786026 |
| rathi | swathi | RSA-304 | | 18.11.2022 21:16:57 | 1668786417 |
| rathi | swathi | RSA-304 | | 19.11.2022 07:27:41 | 1668823061 |
| rathi | swathi | RSA-304 | | 19.11.2022 07:30:26 | 1668823226 |
| rathi | swathi | RSA-304 | | 19.11.2022 11:18:09 | 1668976389 |

Note: Only PSEs containing an RSA key are shown.
Display decryption time

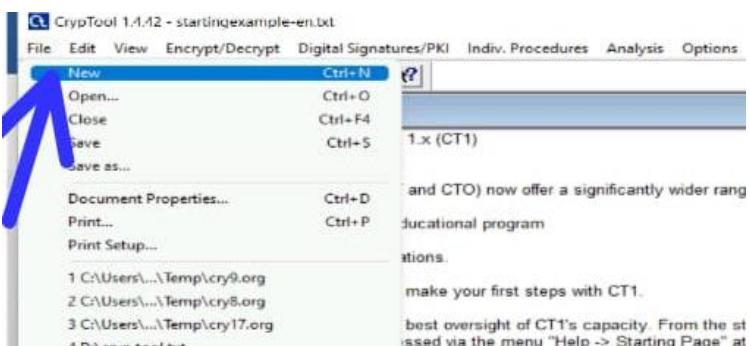
Decrypt Cancel

- Step 5: - Then your message will be decrypted

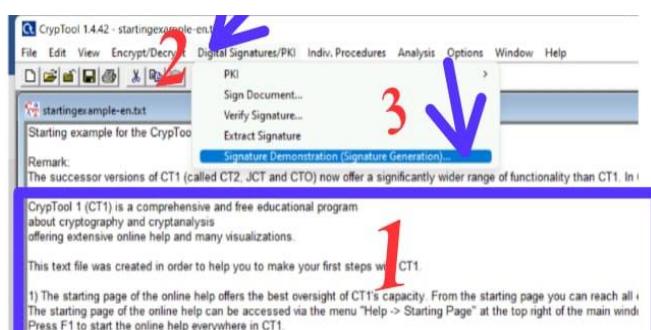


❖ Steps for Digital Signature

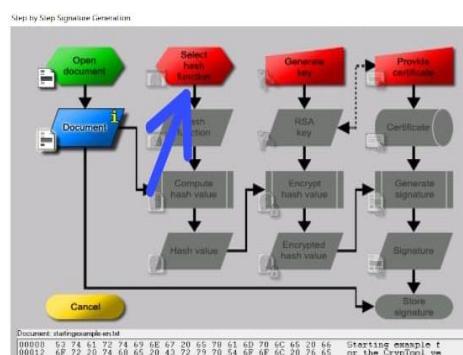
- Step 1: - Go to file Then click on the new



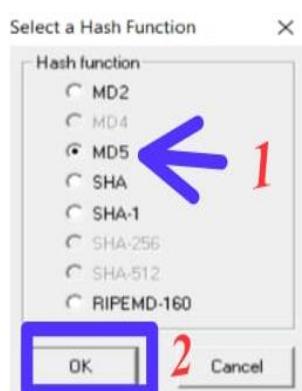
- Step 2: - Type the message & go to digital signature Then click on the signature demonstration



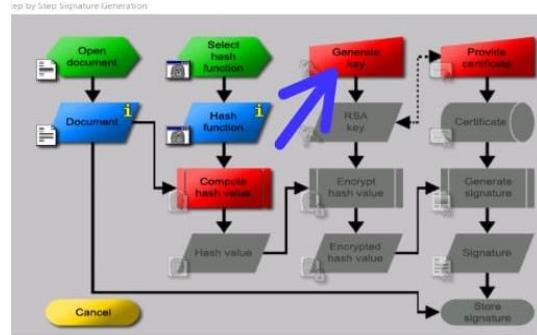
- Step 3: - Click on the select hash function



- 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

Generate RSA Key

Choose two prime numbers p and q . The number $N = pq$ is the public RSA modulus and $\phi(N) = (p-1)(q-1)$ is the Euler phi function. Public key e is coprime to $\phi(N)$. The private key $d = e^{-1} \pmod{\phi(N)}$ is calculated from this.

| | | |
|--|-------------------------------------|--|
| Prime number entry | <input type="text"/> Prime number p | <input type="button" value="Generate prime numbers..."/> |
| | <input type="text"/> Prime number q | |
| RSA parameter | | |
| Length | <input type="text"/> | (public) |
| RSA modulus N | <input type="text"/> | (secret) |
| $\phi(N) = (p-1)(q-1)$ | <input type="text"/> | (secret) |
| Public key e | <input type="text"/> $2^{16}+1$ | |
| Private key d | <input type="text"/> | |
| <input type="button" value="Store key"/> <input type="button" value="Cancel"/> | | |

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

Prime Number Generation

Prime numbers play an important role in modern cryptography. Here you can generate primes within a given value range [lower limit, upper limit].

Amount of prime numbers to be generated

Generate two primes randomly from within the value range(s)
 Generate all primes within the value range set for p

Separator for the display of the primes:

Algorithms for prime number generation

Miller-Rabin Test
 Solovay-Strassen Test
 Fermat Test

Value range of the prime numbers p and q

To be entered independently of each other
 Both are equal (just enter one)

Prime number p

Lower limit: 1
Upper limit: 2

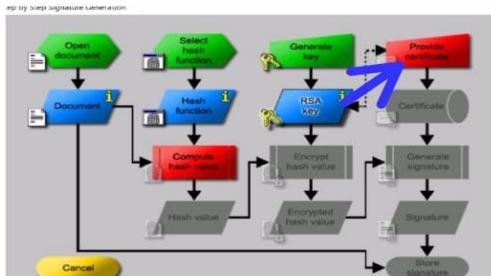
Result: 231633846257977371

Prime number q

Lower limit: 2^150
Upper limit: 2^151

Result: 1434298724673852070

➤ Step 9: - Click on the provide certificate



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

Create Certificate and PSE

Public RSA parameter

Bit length: 304 bit
RSA modulus N: 34795401522451565756725956555411746681920980041133310779009
Public key e: 65537

Personal data for the certificate

Name: Swasuu
First name: reddy 1
Key identifier:
PIN:
PIN verification:

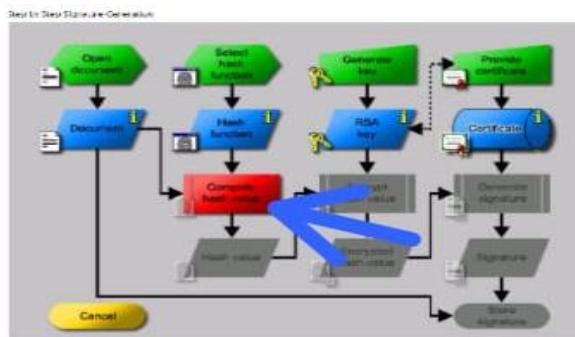
(optional)

Generated names for PSE and certificate

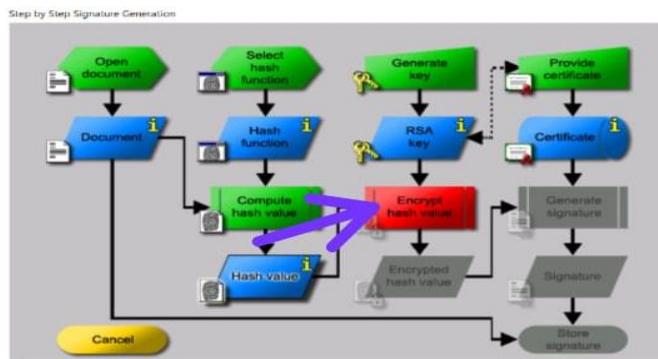
User Key ID: [Swasuu][reddy][RSA-304][1672332813]
Distinguished Name: CN=reddy.Swasuu[1672332813]=cryptool, DC=org

2

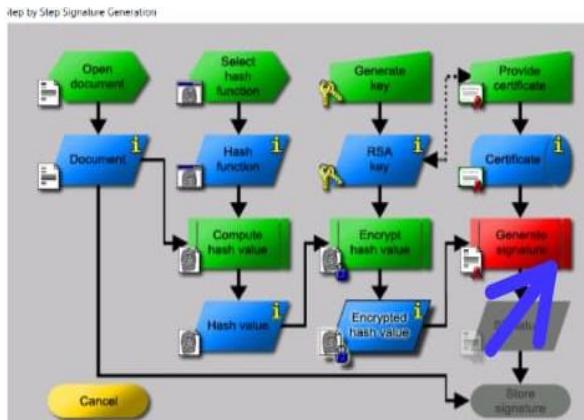
- **Step 11:** - Then click on the compute hash value



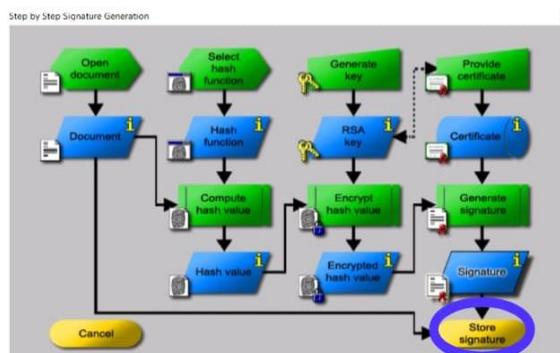
- **Step 12:** - Click on the encrypt hash value



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



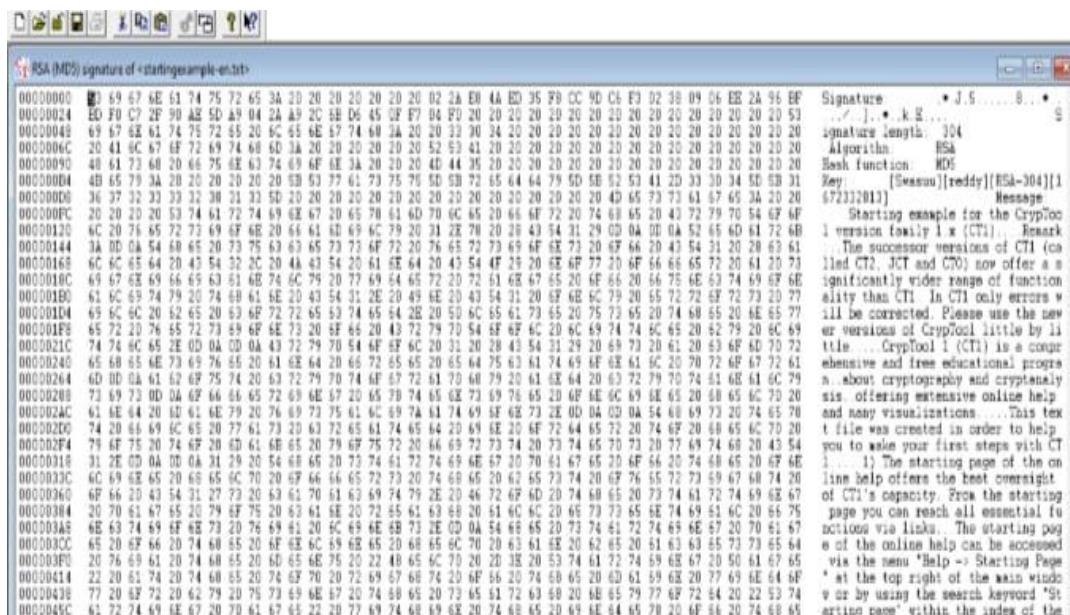
- **Step 14:** - Click on the store signature



➤ **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 until your wifi will show then press ctrl+c

| NUM | ESSID | CH | ENCR | POWER | WPS? | CLIENT |
|-----|---------------------|----|-------|-------|------|--------|
| 1 | (88:3F:67:83:D0:A6) | 13 | WPA-P | 39dB | yes | |
| 2 | Farida H A | 6 | WPA-P | 23dB | no | |
| 3 | (3C:15:FB:D8:B5:50) | 4 | WPA | 22dB | yes | 1 |
| 4 | HUAWEI-B535-D406 | 13 | WPA-P | 14dB | no | |
| 5 | | | | | | |

[+] Scanning... Found 5 target(s), 1 client(s). Ctrl+C when ready ■

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

[+] select target(s) (1-4) separated by commas, dashes or all: [1]

[+] (1/1) Starting attacks against 94:6A:B0:15:41:6A (hug2g858469)

[+] Skipping PMKID attack, missing required tools: hcxdumptool, hcxpcaptool

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

[+] analysis of captured handshake file:

[+] tshark: .cap file contains a valid handshake for 94:6a:b0:15:41:6a

[+] aircrack: .cap file does not contain a valid handshake

[+] Cracking WPA Handshake: Running aircrack-ng with top10000_passwords.txt wordlist

[+] Cracking WPA Handshake: 98.29% ETA: 0s @ 3075.9kps (current key: jasmine3)

[+] Cracked WPA Handshake PSK: north22town

[+] Access Point Name: hug2g858469

[+] Access Point BSSID: 94:6A:B0:15:41:6A

[+] Encryption: WPA

[+] Handshake File: hs/handshake_hug2g858469_94-6A-B0-15-41-6A_2020-08-04T13-59-28.cap

[+] PSK (password): north22town

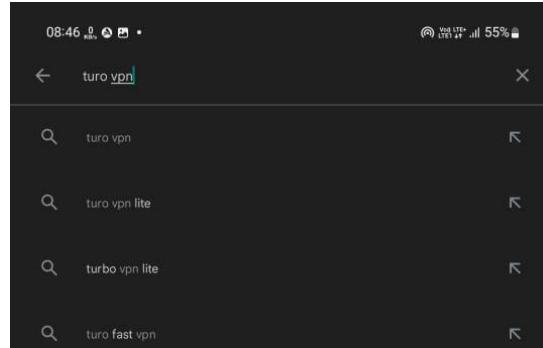
[+] saved crack result to cracked.txt (1 total)

[+] Finished attacking 1 target(s), exiting

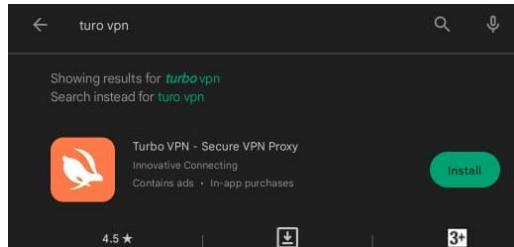
8) Install VPN on mobile and pc and check connection\

❖ On Mobile

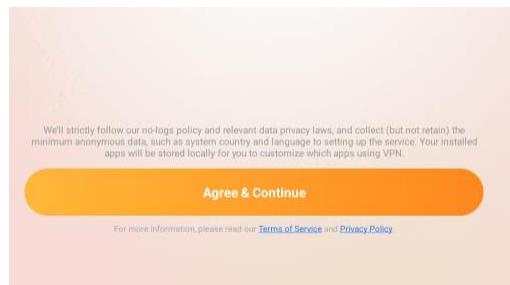
- step 1:-open Playstore and search turbo vpn



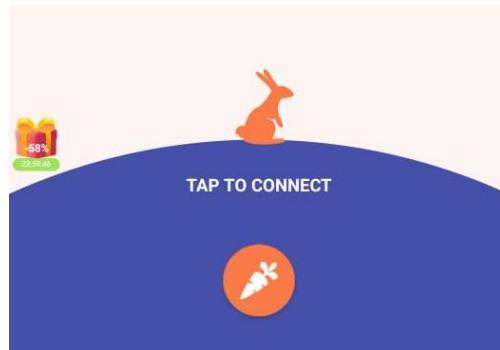
- Step 2:- click install



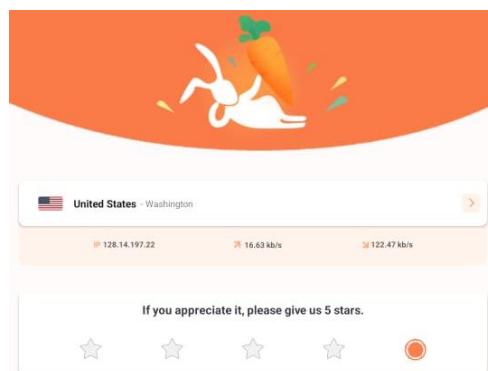
- Step 3:-open turbo vpn and click agree & continu



- Step 4:- press tap to connect



- Step 5:- vpn connected succfully

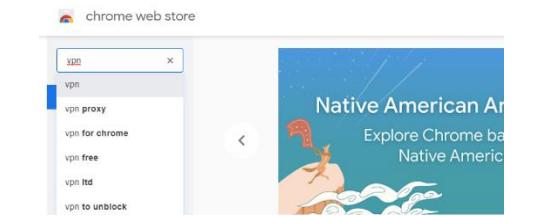


❖ On Computer

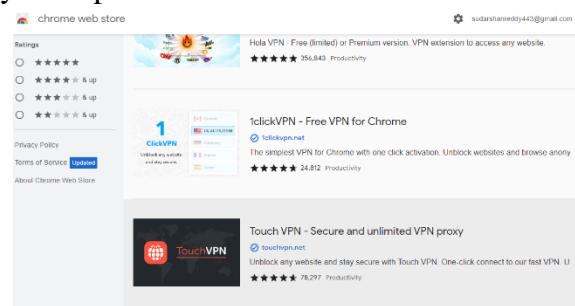
- Step 1:- open chrome browser and search “<https://chrome.google.com/webstore>”



- Step 2:- search vpn on webstore



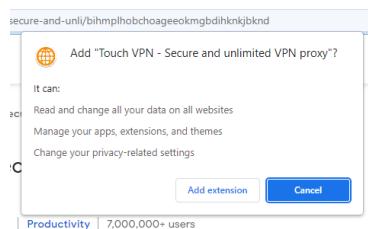
- Step 3:- Click any one vpn



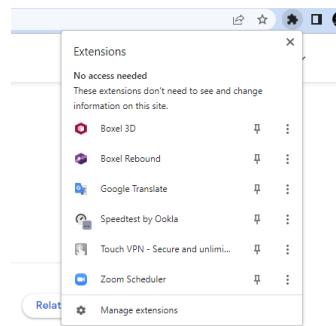
- Step 4:- click add to chrome button to install vpn



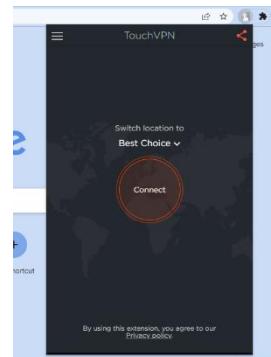
- Step 5:- Click add extension to confirm



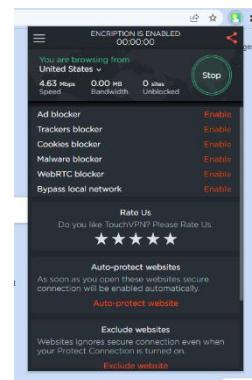
- Step 6:- Click extension icon and click downloaded vpn



- Step 7:- select server and click connect



- Step 8 :- vpn connected successfully \



9) Demonstrate NTFS file system using NTFS permission reporter.

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

<https://www.permissionsreporter.com/>

NTFS Permissions Reporting Software for Windows

You need a visual, interactive software tool to help you manage file system permissions. You need Permissions Reporter - the ultimate network-enabled NTFS permissions reporting tool.

Free download · NTFS Permissions · Share Permissions · Upgrade to Pro

<http://www.cjdev.com/Software/NtfsReports/info>

NTFS Permissions Reporter - Cjdev

NTFS Permissions Reporter is a modern user friendly tool for reporting on directory permissions on your Windows file servers. It lets you quickly see which...

<https://blog.netwrix.com/infrastructure>

Top 11 NTFS Permissions Tools for Smarter Administration

13-Jan-2021 – 1 – NTFS Permissions Reporter Free Edition from Cjdev – 2. Nenmii Effective Permissions Reporting Tool – 3 – Microsofts Access Enum – 4 –

- Step 2: Click on Download Now

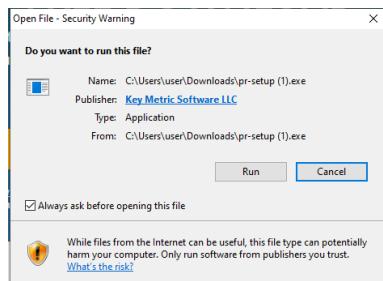


THE NTFS PERMISSIONS ANALYZER FOR WINDOWS

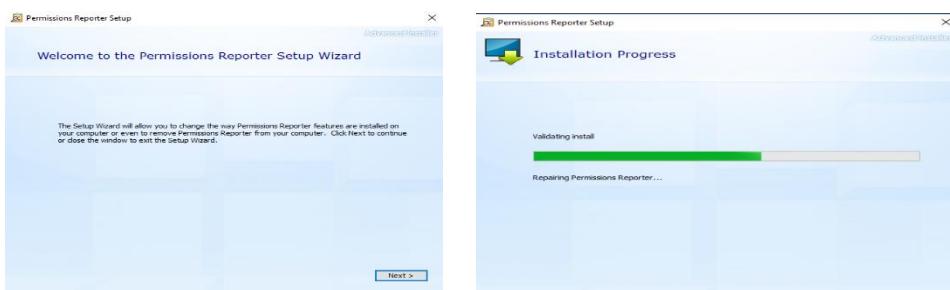
- Step 3: Click on Start Download



- Step 4: Click Run



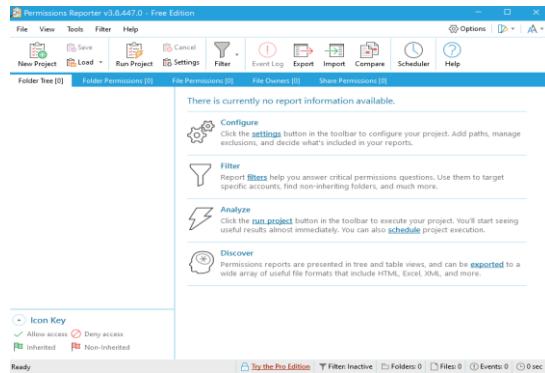
- Step 5: Click on Next



➤ **Step 6:** Click on Close

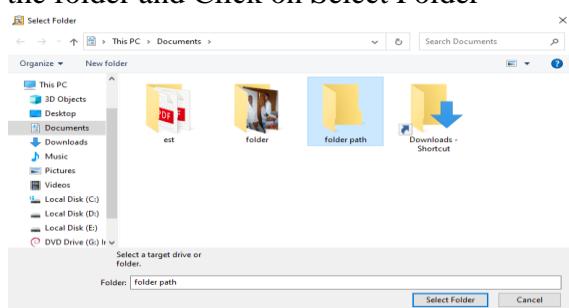


- **Step 7:** open the permission reporter
 ➤ **Step 8:** In Configure, Click on settings

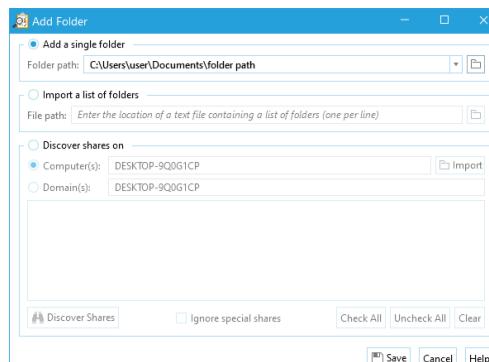


- **Step 9:** In project settings, Select Add Folder

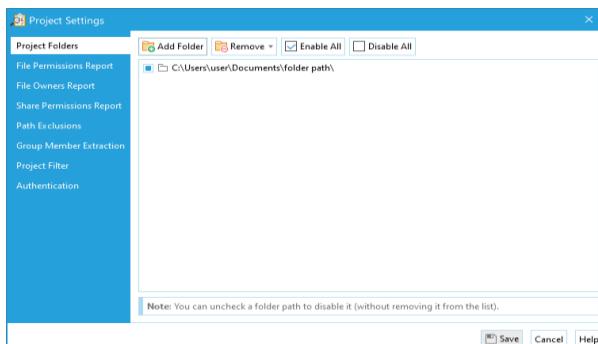
- **Step 10:** Select the folder and Click on Select Folder



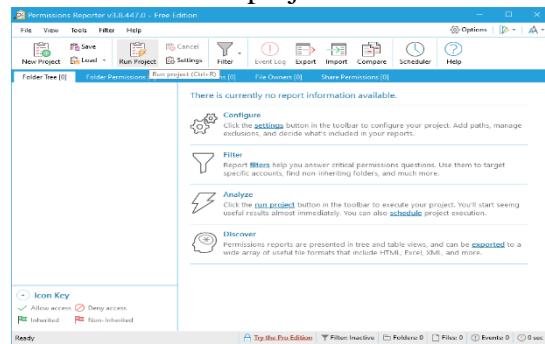
- **Step 11:** Click on Save



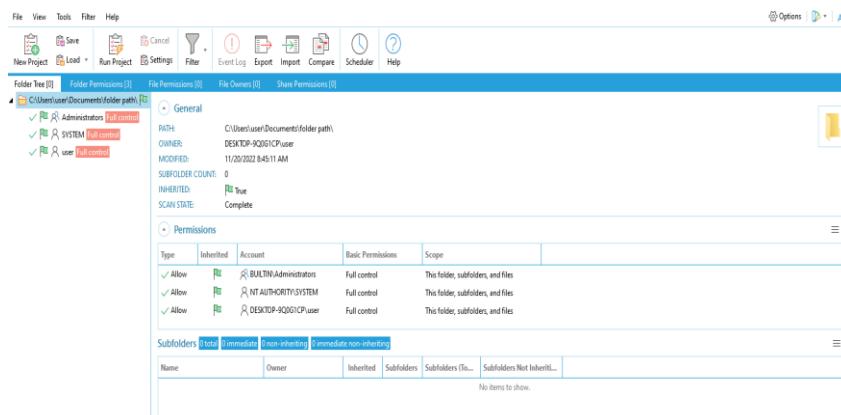
➤ Step 12: Click on Save



➤ Step 13: Click on the run project

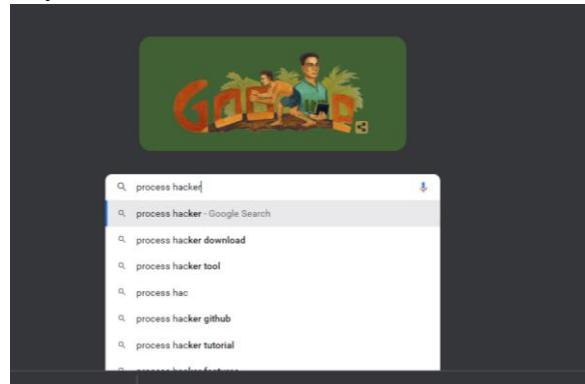


➤ Step 14 : permission of the select folder display on the screen



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

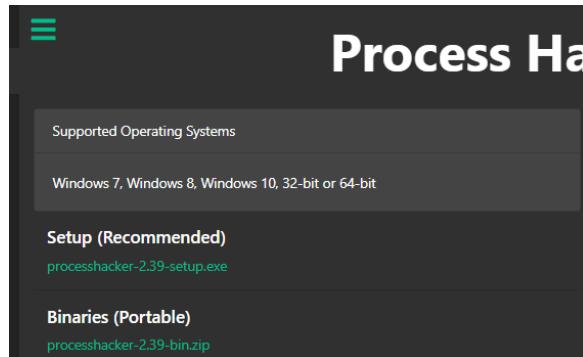
- Step 1: - Go to any browser & Search Process Hacker



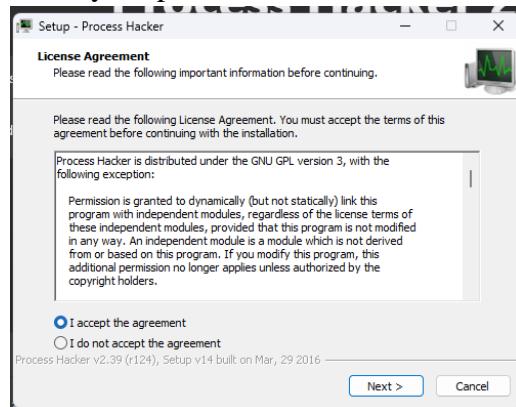
- Step 2: - Search the download process hacker



- 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.

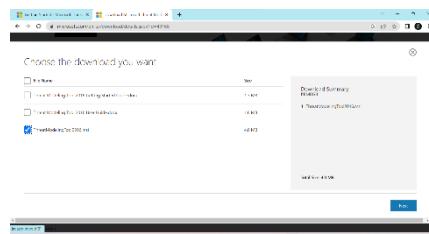
- Step 1 go to any browser search Microsoft threat Modeling tool download



- Step 2 Display the screen Download Microsoft threat Modeling tool 2016



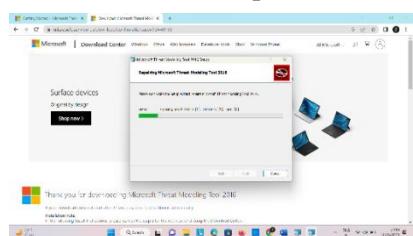
- Step 3 Choose the download you want ThreatModelingTool2016.msi 4.0 click Next



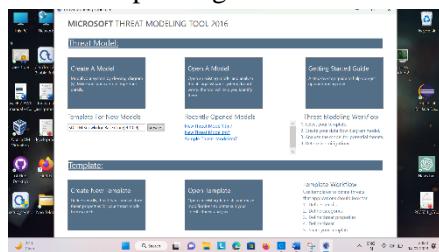
- Step 4 Click Next



- Step 5 finish the installation click next step

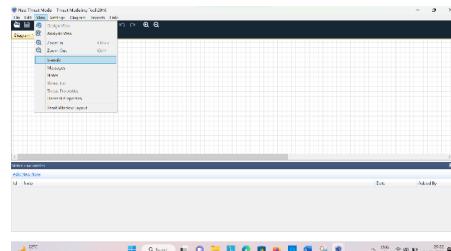


- Step 6 After installation completed go to Threat Model create A Model

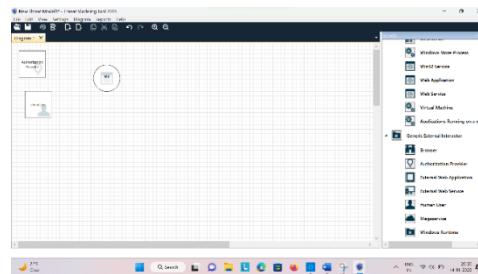


Create application

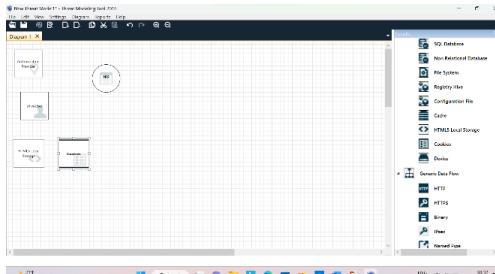
- **Step 7** go to view click stencils display the tools



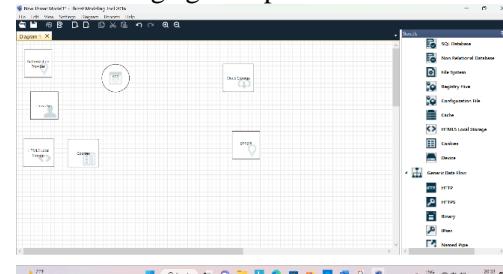
- **Step 8** Take application, Human user, Authentication provider and give the permission



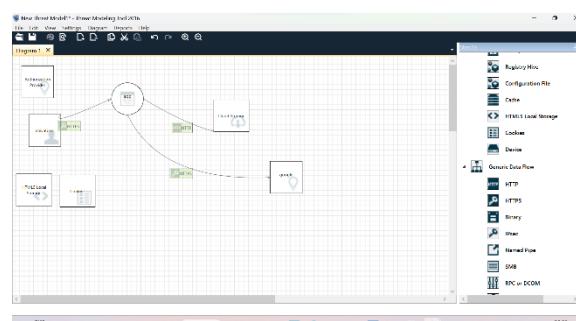
- **Step 9** Take local storage HTML and security cookies



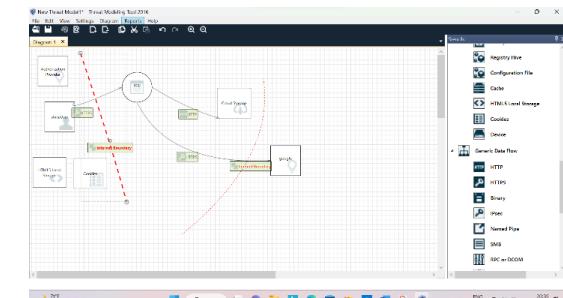
- **Step 10** Take browser and cloud storage give a permission



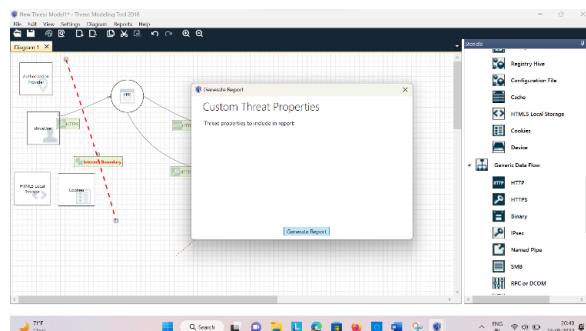
- **Step 11** Assign HTTPS user, google to app and HTTP app to storage



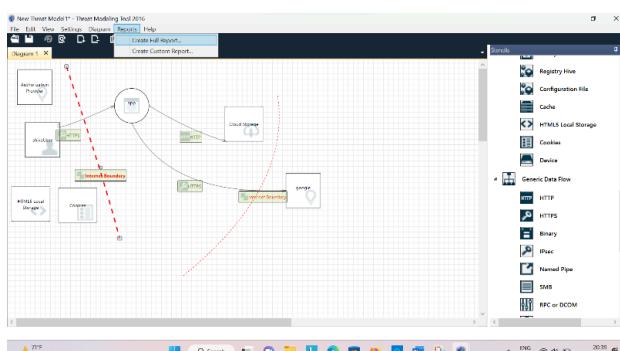
➤ **Step 12** Add Internet Boundary and got reports



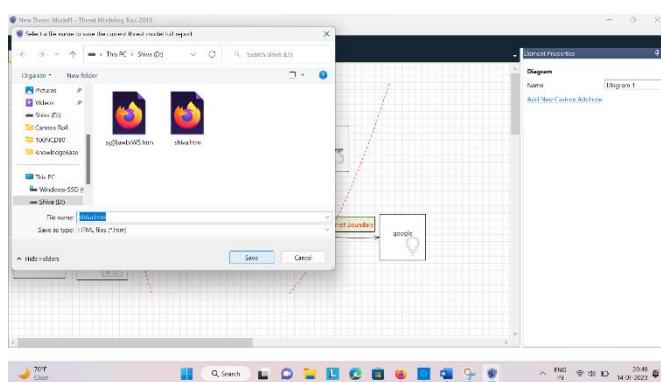
➤ **Step 13** Click Create Full Report



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



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

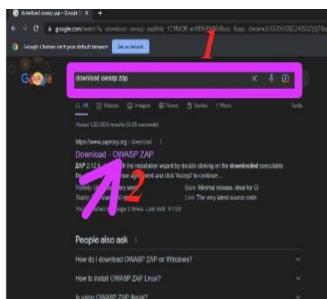


➤ **Step 16** Report will be generated find the vulnerability and threat in your application

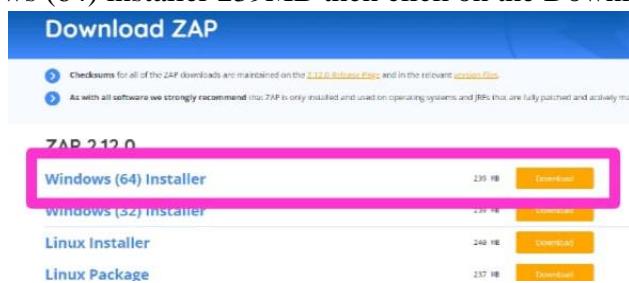
12) Install OWASP ZAP and demonstrate finding vulnerabilities in web application using automated scan & Manual Scan.

*** Automated scan:**

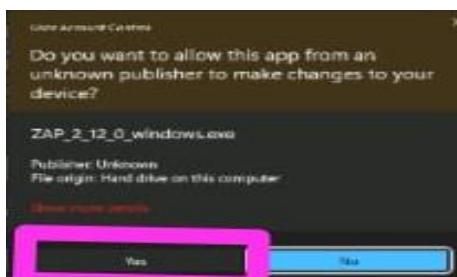
- Step 1: - Go to chrome & search the download OWASP ZAP then click on the download – OWASP ZAP



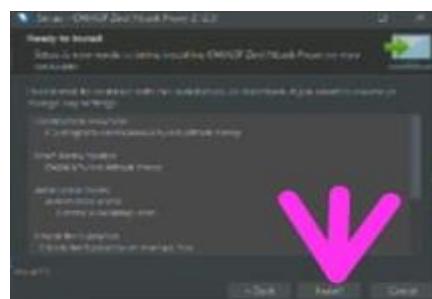
- Step 2: - Select windows (64) installer 239MB then click on the Download



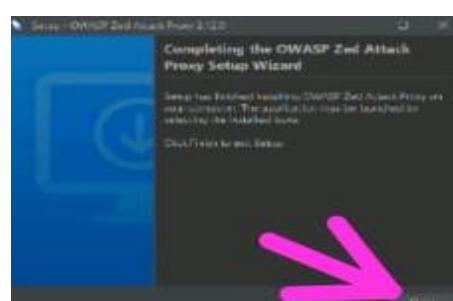
- Step 3: - Now ZAP will be downloaded & double click on ZAP then click on yes



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



- Step 5: - Then click on the finish button

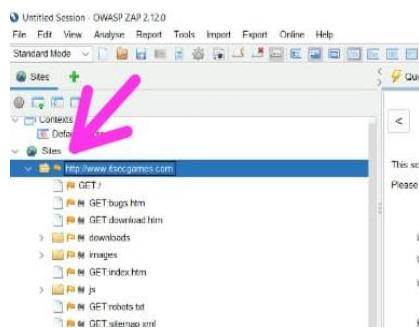


- Step 6: - Open the OWASP ZAP then click on the Automated scan

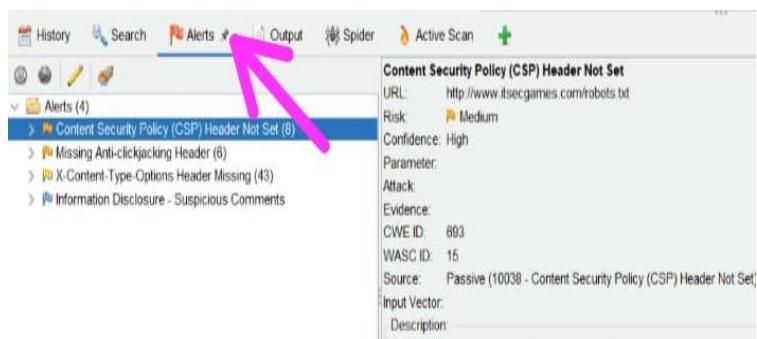
- Step 7: - Paste BW app website URL then click on attack button



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

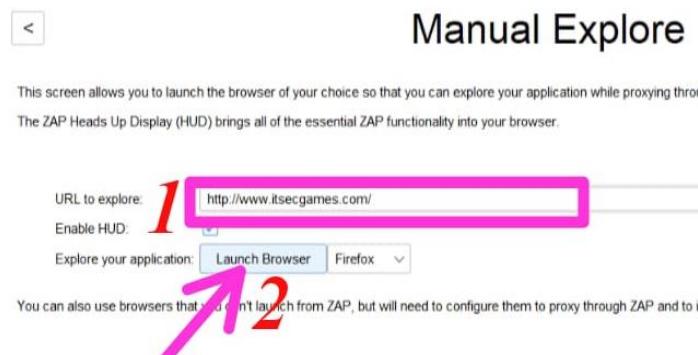


- Step 9: - Now click on Alerts section and analyze type of risk which was exposed by automated scan



***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.

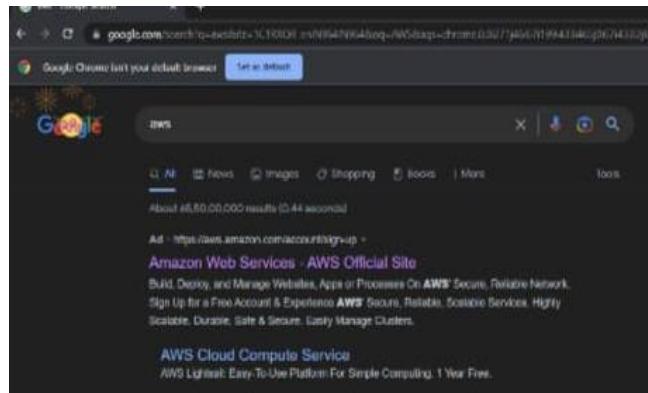
| Content Security Policy (CSP) Header Not Set | |
|--|--|
| URL: | http://www.itsecgames.com/ |
| Risk: | Medium |
| Confidence: | High |
| Parameter: | |
| Attack: | |
| Evidence: | |
| CWE ID: | 693 |
| WASC ID: | 15 |
| Source: | Passive (10038 - Content Security Policy (CSP) Header Not Set) |
| Input Vector: | |
| Description: | Content Security Policy (CSP) is an added layer of security that helps to detect and prevent everything from data theft to site defacement or distribution of malware. CSP provides a way to control what external resources are allowed to load on that page — covered types are JavaScript, CSS, HTML frames, images, and fonts. |
| Other Info: | |

Alerts (10)

- > Content Security Policy (CSP) Header Not Set
 - > Cross-Domain Misconfiguration (6)
 - > Missing Anti-clickjacking Header
 - > Server Leaks Version Information via "Server" HTTP Response Header
 - > Strict-Transport-Security Header Not Set (15)
 - > Timestamp Disclosure - Unix (14)
 - > X-Content-Type-Options Header Missing (16)
 - > Information Disclosure - Suspicious Comments
 - > Re-examine Cache-control Directives (4)
 - > Retrieved from Cache (20)

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

Sign up for AWS

Root user email address
Used for account recovery and some administrative functions.

AWS account name
Choose a name for your account. You can change this name in your account settings after you sign up.

Verify email address

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

Sign up for AWS

Confirm you are you

Making sure you are secure — it's what we do.

We sent an email with a verification code to [\(not you?\)](mailto:swasuureddy143@gmail.com)

Enter it below to confirm your email.

Verification code

Verify

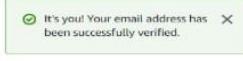
Resend code

Didn't get the code?
• Codes can take up to 5 minutes to arrive.
• Check your spam folder.

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

Sign up for AWS

Create your password



Your password provides you with sign in access to AWS, so it's important we get it right.

Root user password

Confirm root user password

Continue (step 1 of 5)

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

Who should we contact about this account?

Full Name
Swathi N

Phone Number
+91 9876543210

Country or Region
India

Address
Apartment, suite, unit, building, floor, etc.

City
chikkaballapur

State, Province, or Region
karnataka

Postal Code
562101

Customers with an Indian contact address are served by Amazon Web Services India Private Limited, the local seller for AWS services in India.

I have read and agree to the terms of the AWS Customer Agreement [\[Link\]](#)

Continue (step 2 of 5)

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

Credit or Debit card number


more options for credit and debit cards. To learn more about payment options, review our FAQ.

Expiration date
October 2026

Cardholder's name
N PAVITHRA

CVV

Billing address

Use my contact address
behind cocoon market road vaganadra chikkaballapur karnataka 562101 IN

Use a new address

Do you have a PAN?
Pan Card number (PAN) is a ten-digit alphanumeric number issued by the Indian Income Tax department. The PAN number is printed on the front of your PAN card.

Yes

No

You can go on the Tax Settings Page on Billing and Cost Management Console to update your PAN information.

Verify and Continue (step 3 of 5)

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

MasterCard SecureCode. 

| | |
|-------------------------|------------------------|
| Merchant | : AMAZON |
| Transaction Date & Time | : 01-Jan-2023 18:10:30 |
| Transaction Amount | : ₹ 2.00 |
| Card Number | : xxxx xxxx xxxx 7433 |

Authenticate Payment
We have sent an OTP to your mobile number 8880200096

Enter One Time Password (OTP)
899223

Make Payment

[Cancel and Go back to merchant](#)

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

Sign up for AWS

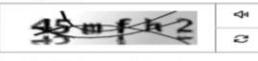
Confirm your identity

Before you can use your AWS account, you must verify your phone number. When you continue, the AWS automated system will contact you with a verification code.

How should we send you the verification code?
 Text message (SMS)
 Voice call

Country or region code
India (+91)

Mobile phone number

Security check


Type the characters as shown above
45mft2

Send SMS (step 4 of 5)

- Step 10: - Then enter the verification code

Sign up for AWS

Confirm your identity

Verify code

5313

Continue (step 4 of 5)

- Step 11: - Then click on complete sign up

Sign up for AWS

Select a support plan

Choose a support plan for your business or personal account. Compare plans and pricing examples
 You can change your plan anytime in the AWS Management Console.

| | | |
|---|--|---|
| Basic support - Free Recommended for new users just getting started. • Direct self-service access to AWS Support. • Fair account and usage limits. • Access to Personal Support and Trusted Advisor. | Developer support - From \$29/month Recommended for individuals experimenting with AWS. • Email access to AWS Support. • 24x7 Developer-hour response times. | Business support - From \$100/month Recommended for individuals with frequent workloads on AWS. • 24x7 Business-hour support via email, phone, and ticket. • 4-hour response times. • Full set of Trusted Advisor recommendations. |
|---|--|---|

Need Enterprise level support?
From \$15,000 a month you will receive 15-minute response times and concierge-style experience with an assigned Technical Account Manager. Learn more

Complete sign up

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



Congratulations

Thank you for signing up for AWS.
ing your account, which should only take a few minutes. You will recei
this is complete.

Go to the AWS Management Console

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

Sign in Events Explore More Q

Sign In to the Console

Check your tax details for accurate invoicing >>

Contact Sales

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

Next

Sign in

Root user
Account owner that performs tasks requiring unrestricted access. Learn more

IAM user
User within an account that performs daily tasks. Learn more

Account ID (12 digits) or account alias

Next

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

Security check

Type the characters seen in the image below

syfrg6

Submit

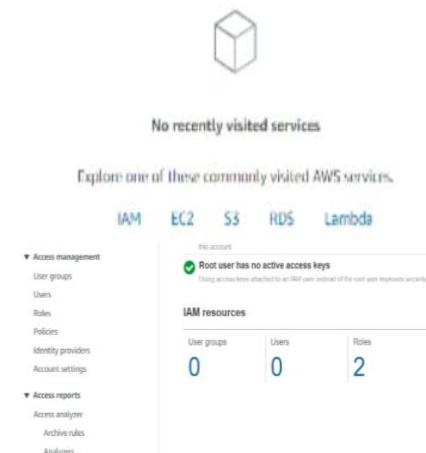
- Step 16: - Enter your password then click on sign in option

Root user sign in

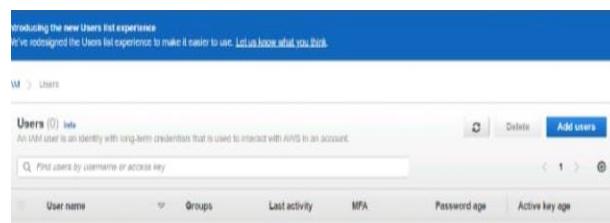
Email: swasureddy143@gmail.com

| | |
|--|----------------------------------|
| Password | Forgot password? |
| <input type="password" value="*****"/> | |
| <input type="button" value="Sign in"/> | |

- 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

Multiple users at once with the same access type and permissions. Learn more

User name*:

Add another user

Access type: Do not set programmatic access. If you choose very programmatic access, it does NOT prevent users from accessing the console using AWS keys or auto-generated passwords are provided in the next step. Learn more

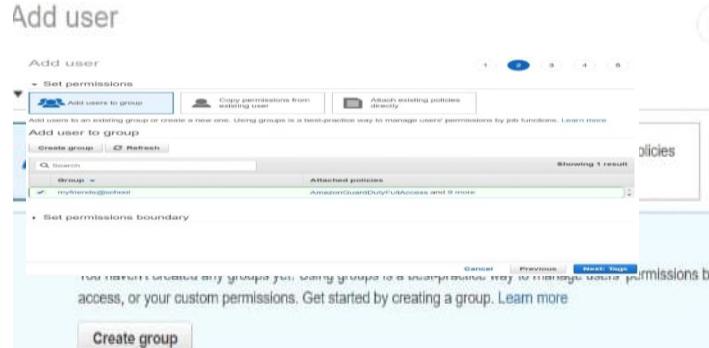
AWS credential type* Access key - Programmatic access Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other AWS services.

Password - AWS Management Console access Enables a password that allows users to sign-in to the AWS Management Console.

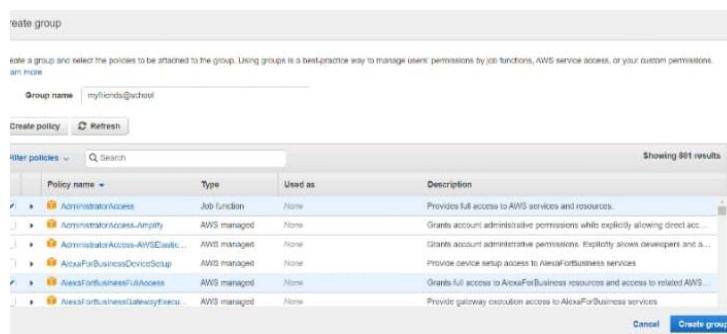
Console password* Autogenerated password Custom password Show password

Require password reset Users must create a new password at next sign-in. Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

- Step 21: - Click on create group

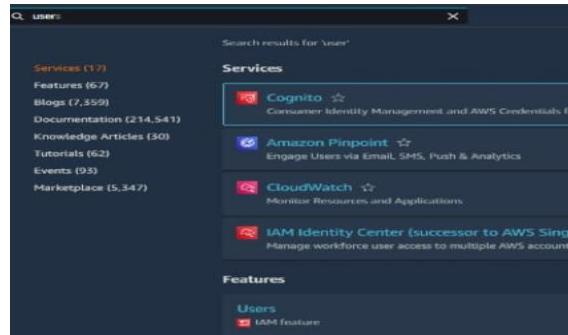


- Step 22: - Enter the group name & Give a policies then click on create group



- 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

Manage MFA device

Name*
chandana
Maximum 128 characters. Use alphanumeric and '+' = , @ - _ characters.

Choose the type of MFA device to assign:

- Virtual MFA device
Authenticator app installed on your mobile device or computer
- Security key
Authenticate by using a FIDO security key, such as Yubikey
- Other hardware MFA device
Hardware TOTP token

For more information about supported MFA devices, see AWS Multi-Factor Authentication

Cancel 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

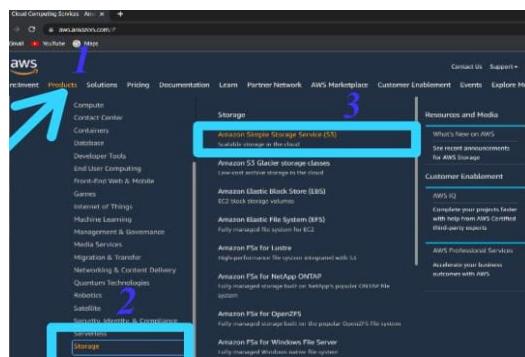


- Step 30: - Enter the numeric code from the authentication into the AWS console. Then wait for a new code to appear in the authenticator. Enter the second code. Then click on “Assign MFA”

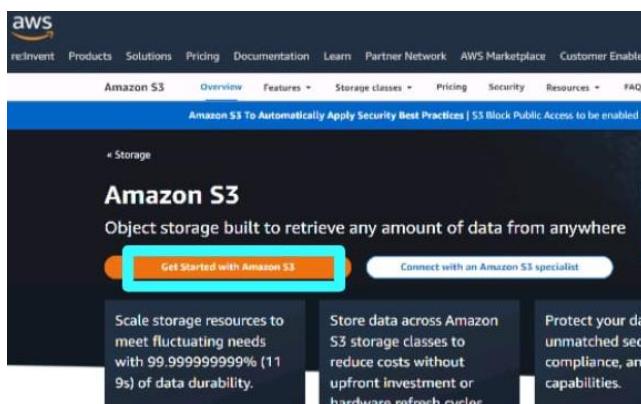


14) Demonstrate the creation of S3 bucket service in AWS & store some files in S3 bucket.

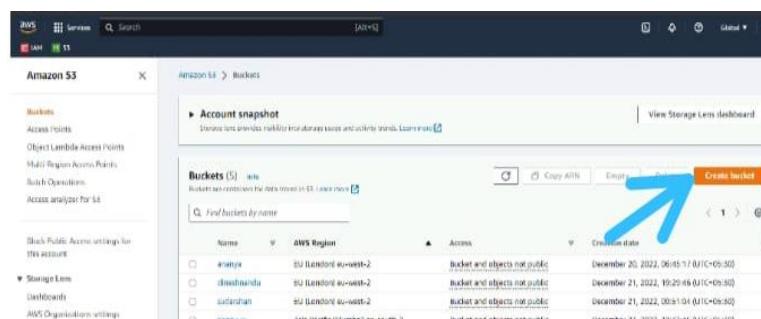
- Step 1: - After login, go to products in AWS & select the storage option then click on the Amazon simple storage service(S3)



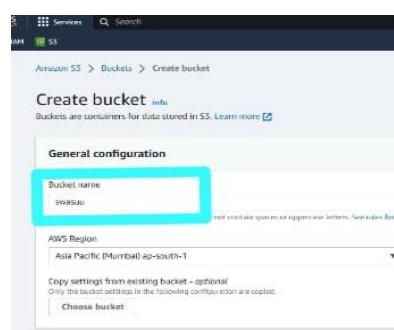
- Step 2: - Click on Get started with amazon S3



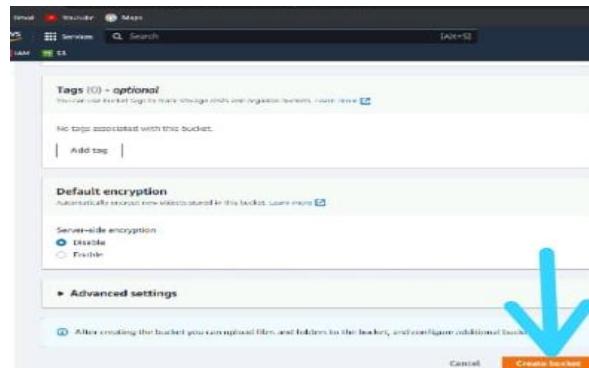
- Step 3: - Then click on create bucket



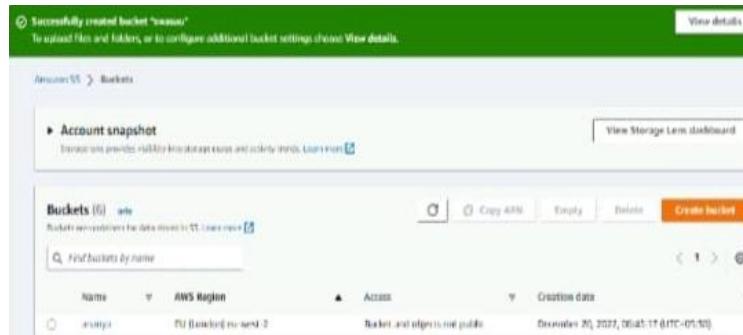
- Step 4: - Enter the bucket name then scroll down



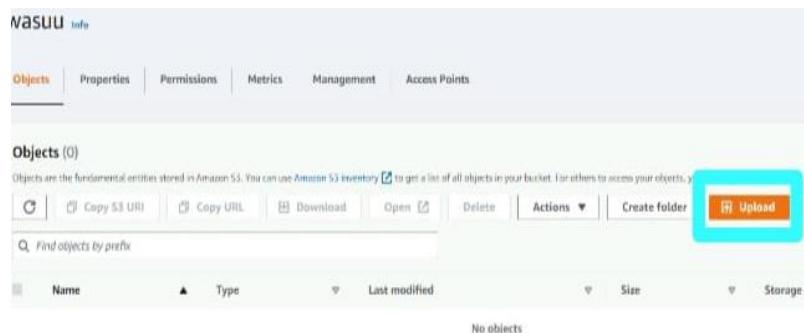
- Step 5: - Click on create bucket



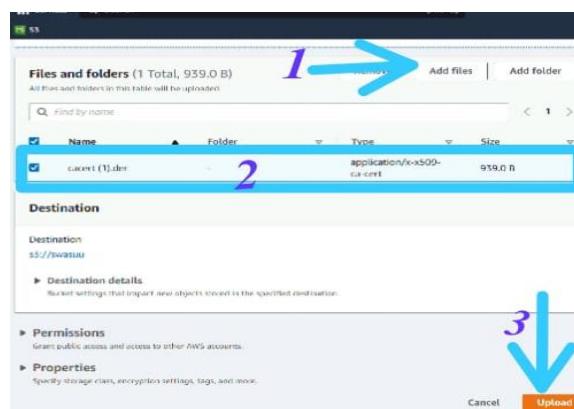
- Step 6: - Then bucket will be created



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



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

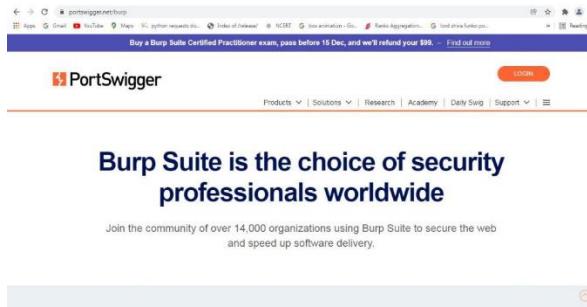


- Step 9:- Then file will be uploading to S3 bucket.

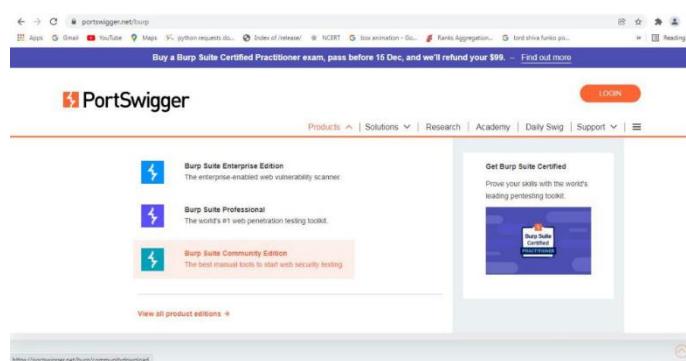
The screenshot shows a web-based interface for managing an S3 bucket. At the top, a green header bar displays the message "Upload succeeded" and "View details below". Below this, a summary table provides an overview of the upload: "Destination" is listed as "s3://sudarshan" and "Status" is "Succeeded" with a green checkmark icon. A note states, "The information below will no longer be available after you navigate away from this page." The main content area is titled "Files and folders" and shows a single item: "cacert (7).der" with a size of "939.0 B". The "Configuration" tab is also visible at the top of this section.

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

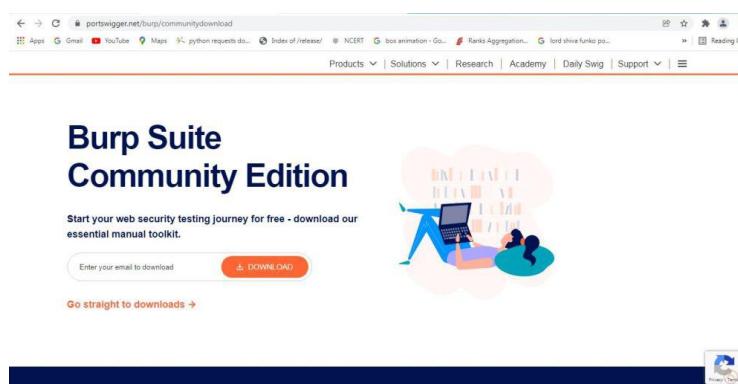
- **Step 1:** Visit the [official Burp Suite website](https://portswigger.net/burp) using any web browser.



- **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.

Professional / Community 2021.10.3

Stable

02 December 2021 at 15:14 UTC



| | | | |
|------------------------------|------------------|----------|----------------|
| Burp Suite Community Edition | Windows (64-bit) | Download | show checksums |
| Burp Suite Professional | | | |
| Burp Suite Community Edition | | | |

well as several minor bug fixes.

Professional / Community 2021.10.3

Stable

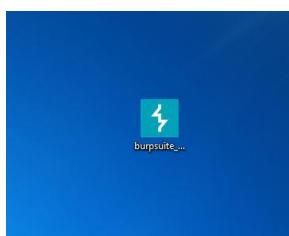
02 December 2021 at 15:14 UTC



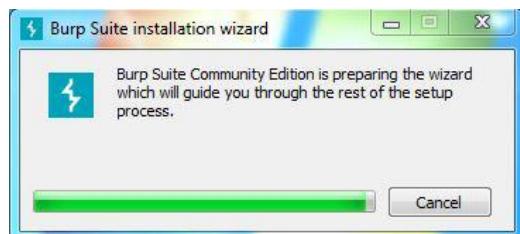
| | | | |
|------------------------------|------------------|----------|----------------|
| Burp Suite Community Edition | Windows (64-bit) | Download | show checksums |
| JAR | | | |
| Linux (64-bit) | | | |
| MacOS (Intel) | | | |
| Windows (64-bit) | | | |

This release provides a security patch, as well as several minor bug fixes.

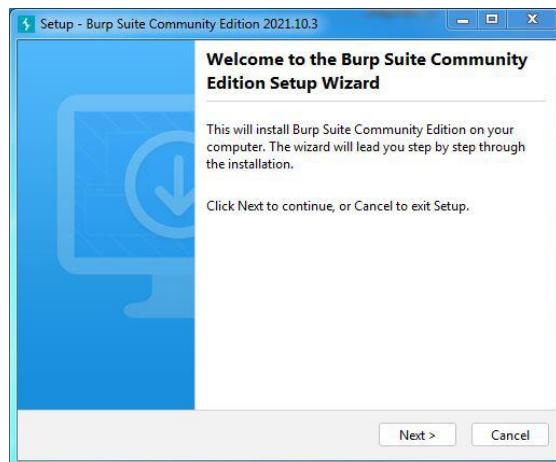
- **Step 5:** Now check for the executable file in downloads in your system and run it.



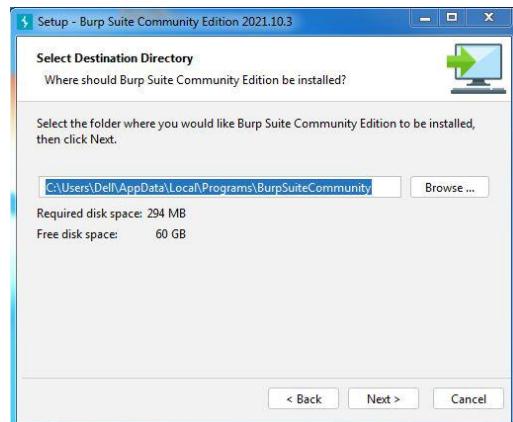
- **Step 7:** Loading of Installation Wizard will appear which will take a few seconds.



- **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.



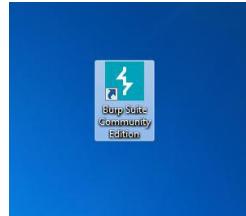
➤ **Step 11:** installation process will start and will hardly take a minute to complete the installation.



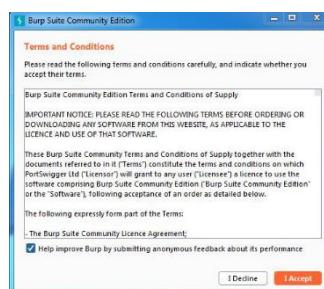
➤ **Step 12:** Click on Finish



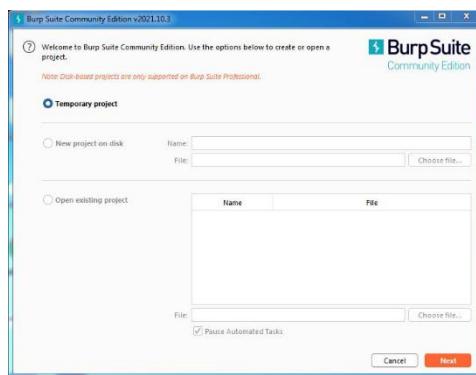
Step 13: Burp suite is successfully installed on the system and an icon is created on the desktop



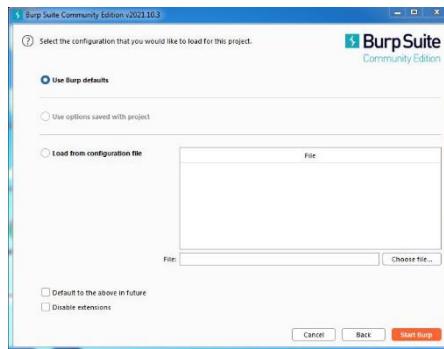
Step 14: Run the software, Click on I Accept.



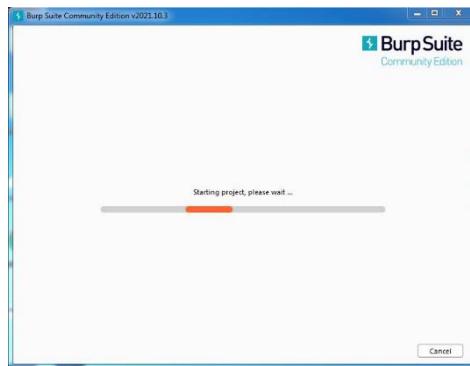
➤ **Step 15:** Choose click Next.



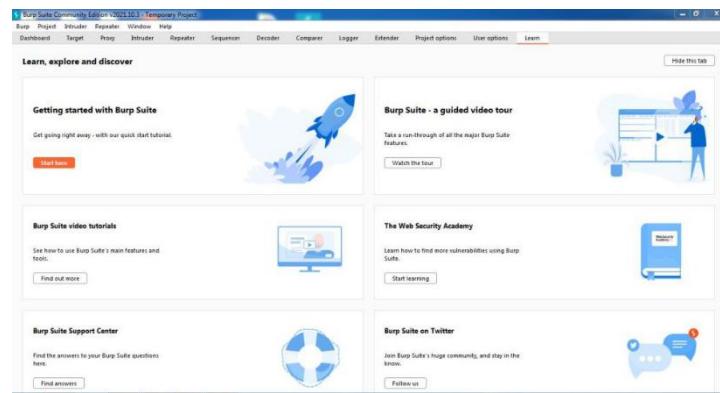
➤ **Step 16:** click on Use Burp Defaults.



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

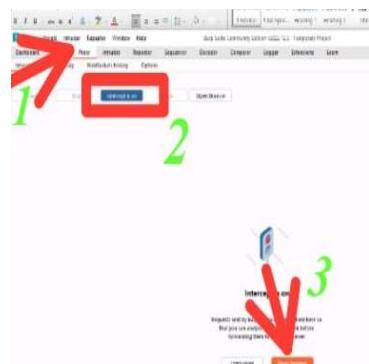


➤ **Step 18:** Finally new project window will appear.



❖ **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



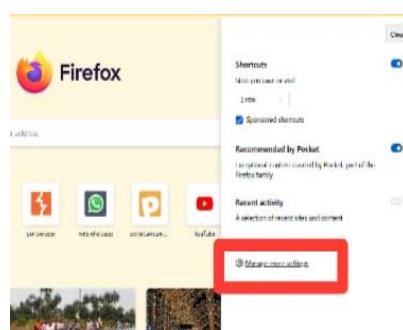
- Step 4: - Search the <http://Burpsuite> then click on the CA certificate
- Step 5: - Then CA certificate will be downloaded



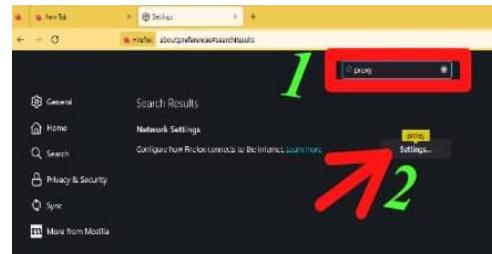
- Step 6: - Open the fire fox then go to settings



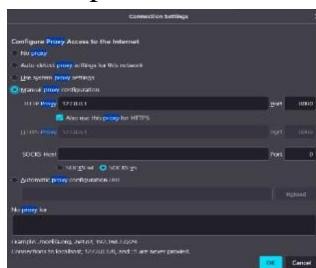
- Step 7: - Then click on the manage more settings



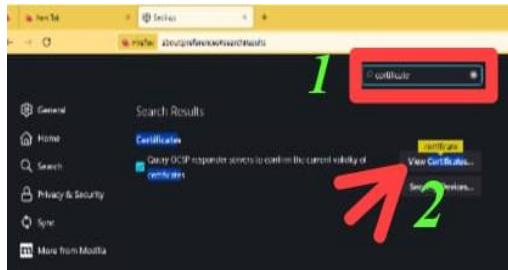
- Step 8: - Search the proxy then click on the proxy settings



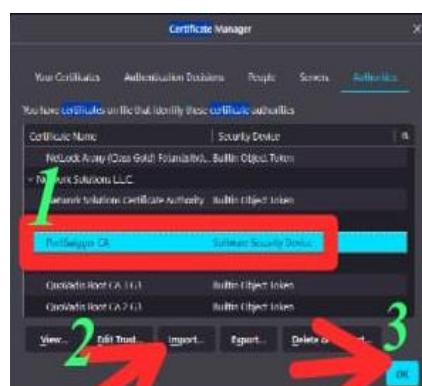
- Step 9: - Choose the manual proxy configuration & enter the HTTP proxy and Port then click on ok option EX: - 127.0.0.1 & 8080



- 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

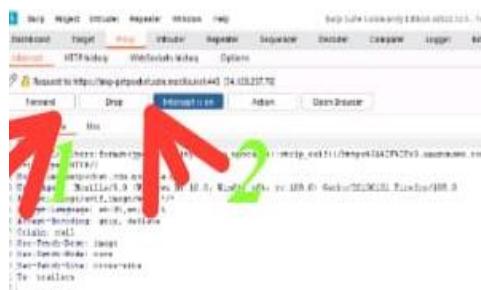


- Step 12: - Open the fire fox then search the any website name\

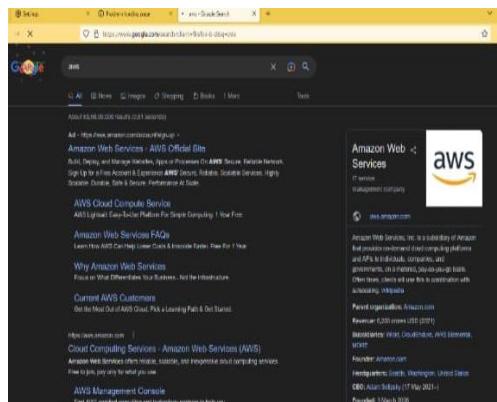
- Step 13: - Now we can't reach the website, So



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

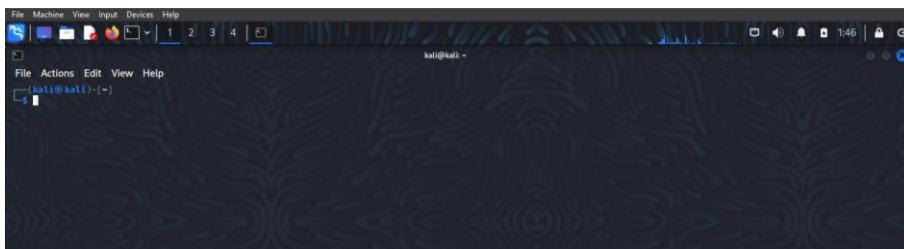


- Step 15: - Now we can reach the website

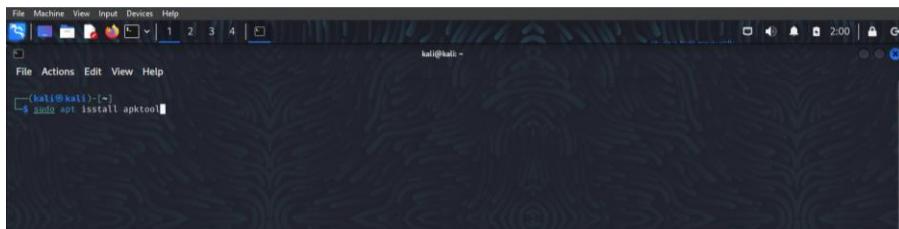


16) Install the Apktool on your Virtual machine and perform reverse engineering on the DIVA Android application.

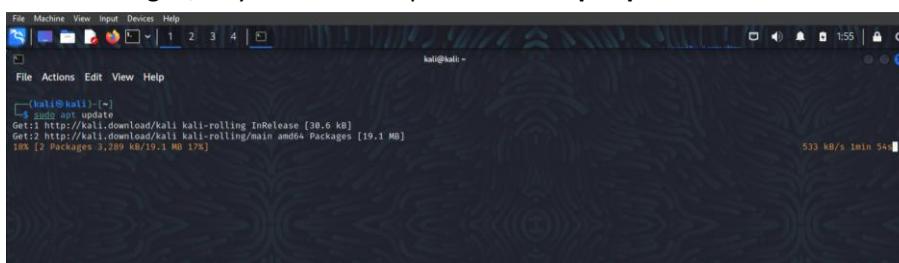
- Step 1:- Open terminal in kali linux



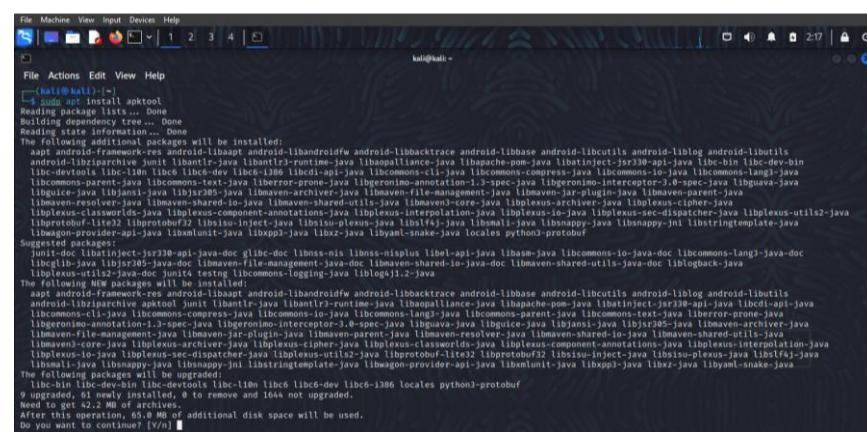
- Step 2 :- Install apktool using this command “**sudo apt install apktool**” & press Enter button



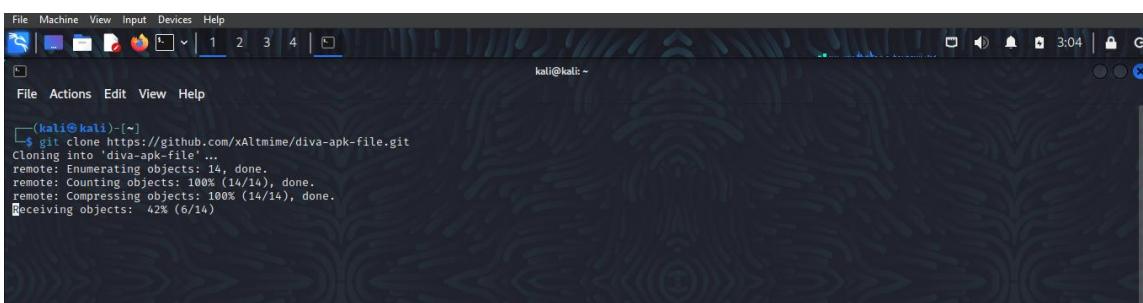
- If installation not begin / any error show update “**sudo apt update**”



- Step 3:- Wait until 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”

```
File Machine View Input Devices Help
3:41
File Actions Edit View Help
kali@kali: ~/diva-apk-file
(kali㉿kali)-[~]
$ cd diva-apk-file
(kali㉿kali)-[~/d
diva-apk-file]
$ ls
DivaApplication.apk LICENSE README.md
(kali㉿kali)-[~/d
iva-apk-file]
$
```

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

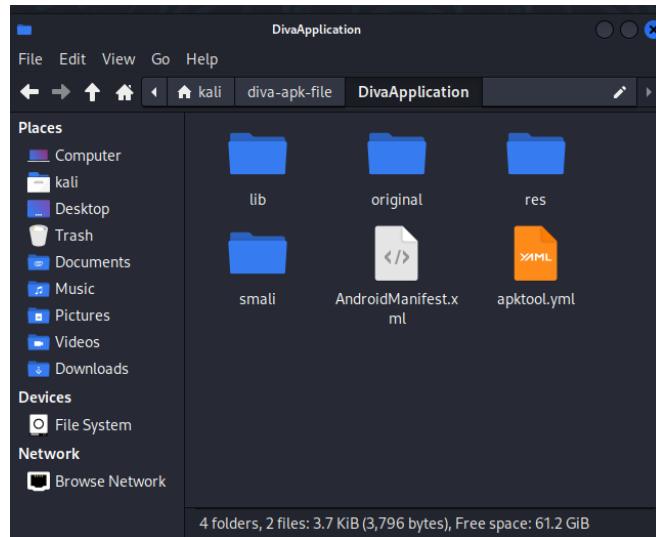
```
File Machine View Input Devices Help
[ 1 2 3 4 ] kali@kali:~/diva-apk-file
File Actions Edit View Help
-kali@kali:~/diva-apk-file
apktool usage:
  -o,--output <dir>      The name of folder that gets written. Default is apk.out
  -p,--path <dir>         Uses framework files located in <dir>.
  -r,--no-res             Do not decode resources.
  -s,--no-src             Do not decode sources.
  -t,--frame-tag <tag>   Uses framework files tagged by <tag>.
usage: apktool [build] [options] <app-path>
  -f,--force-all          Skip changes detection and build all files.
  -o,--output <dir>       The name of apk that gets written. Default is dist/name.apk
  -p,--path <dir>         Uses framework files located in <dir>

For additional info, see: https://ibotpeaches.github.io/Apktool/
For smali/baksmali info, see: https://github.com/JesusFreke/smali

(kali㉿kali)-[~/diva-apk-file]
$ ls
DivApplication.apk LICENSE README.md

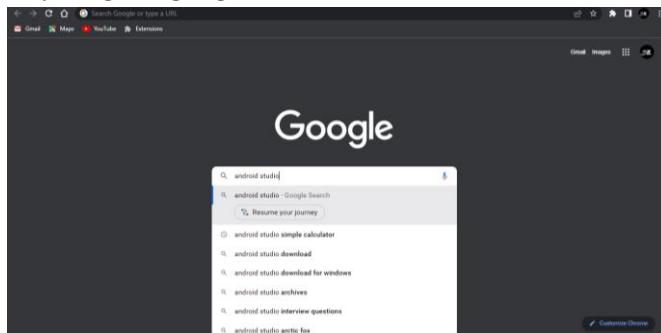
(kali㉿kali)-[~/diva-apk-file]
$ apktool d DivApplication.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1 on DivaApplication.apk
I: Loading source code...
I: Decoding AndroidManifest.xml with resources ...
I: Loading resource table from file: /home/kali/.local/share/apktool/framework/1.apk
I: Regular manifest package ...
I: Decoding file-resources ...
I: Decoding values */* XMLs ...
I: Baksmaling classes.dex ...
I: Copying assets and libs ...
I: Copying unknown files...
I: Copying original files ...
```

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

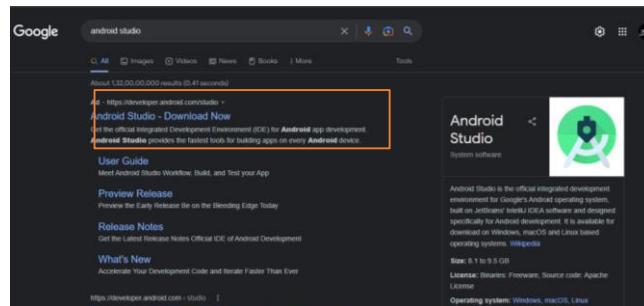


17) Download and install the android studio and create a AVD

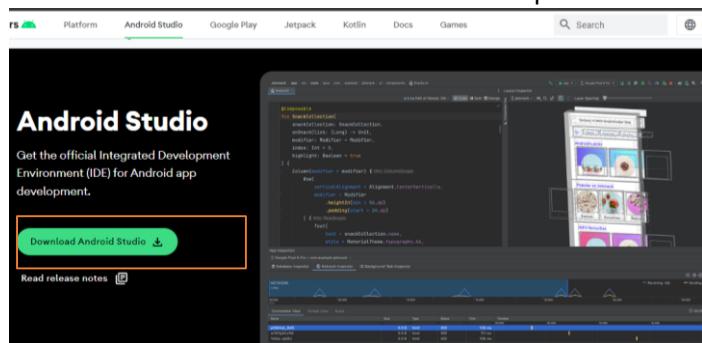
- Step 1:- go to google and search android studio



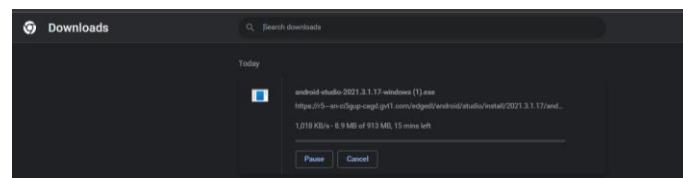
- Step 2:- Click on Android Studio – download now option



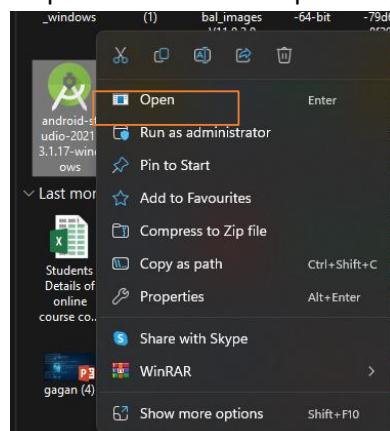
- Step 3:-Now click download android studio option & click terms and conditions and press Download android studio Dolphin



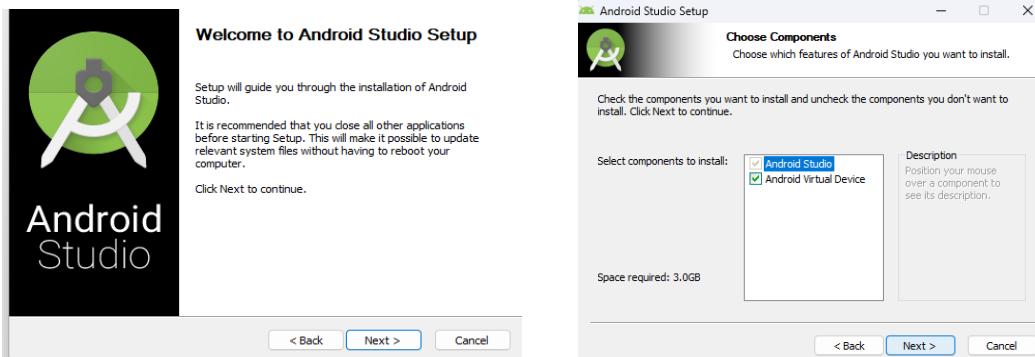
- Step 4:- Wait until download complete



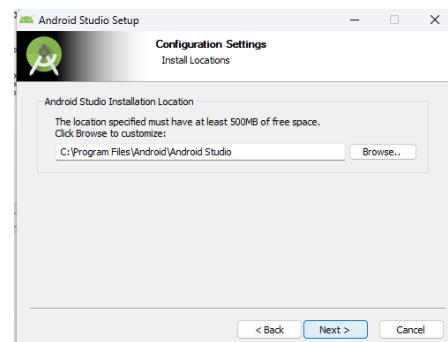
- Step 5:- After complete the download open the software



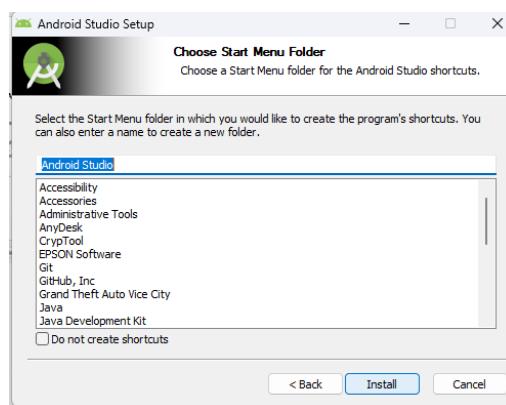
- Step 6:- Click next button and Choose Components and click next.



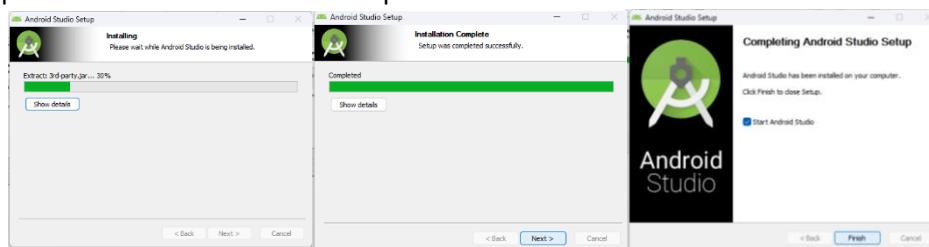
- Step 7:- Select File save location and click next.



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



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



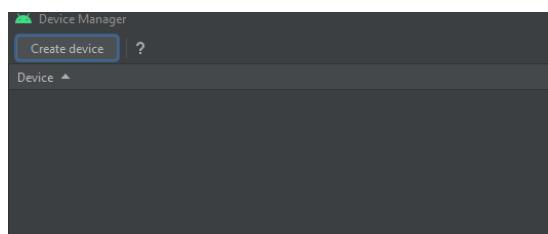
- Step 10:- Click on more Actions



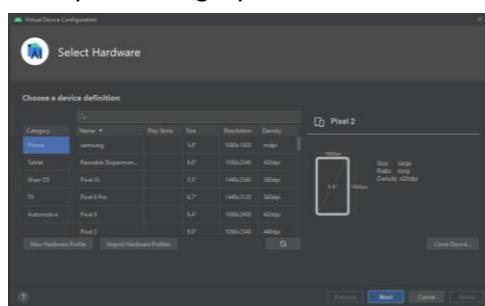
- Step 11:- Now click on Virtual Device Manager



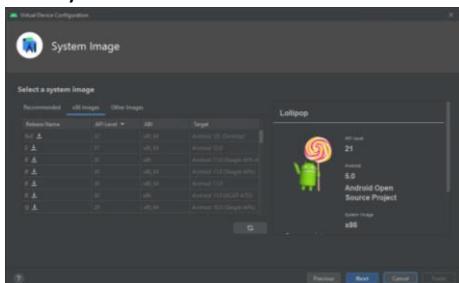
- Step 12:- Click on create device



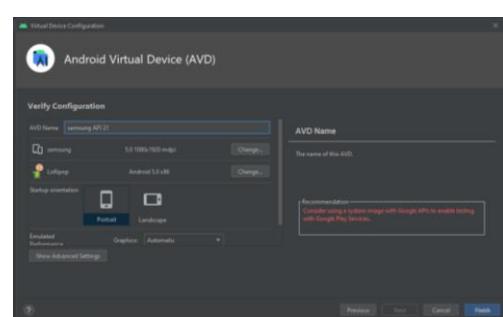
- Step 13:-select any one category & model then click next



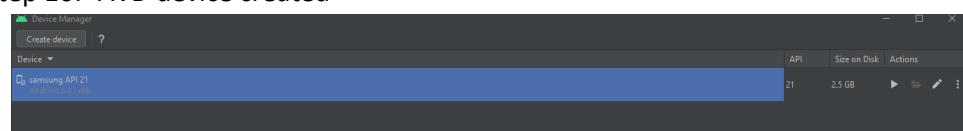
- Step 14:- select any one android version and click next



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

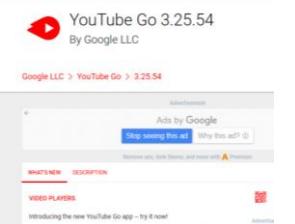


- Step 16:- AVD device created

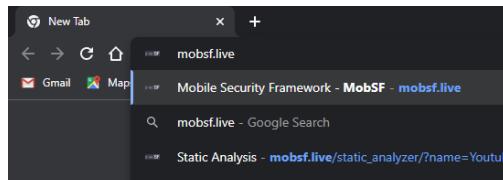


18) Scan any 5 android apps and analyse the report's using MobSF

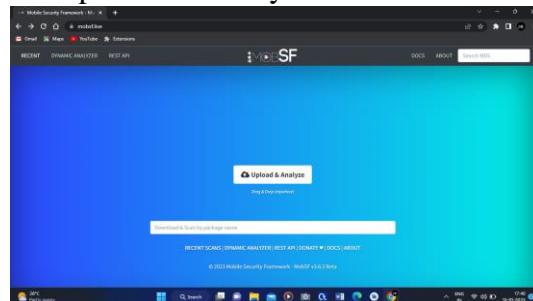
- Step 1:- go to any one browser and download any 5 android apps like “**youtube go, Instagram lite,fb lite, snaptube,dr driving**”



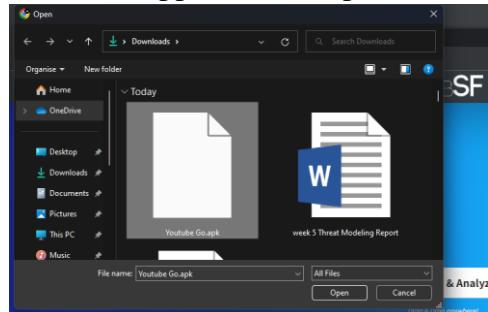
- Step 2:- after download the apps open any browser and search “**mobsf.live**”



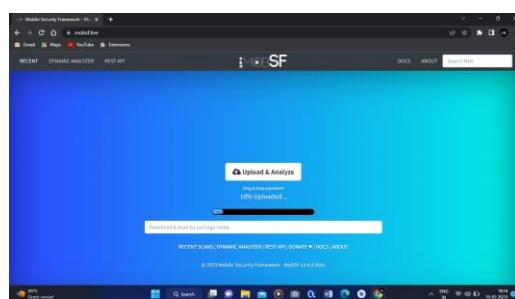
- Step 3:- Then click on upload and analyse



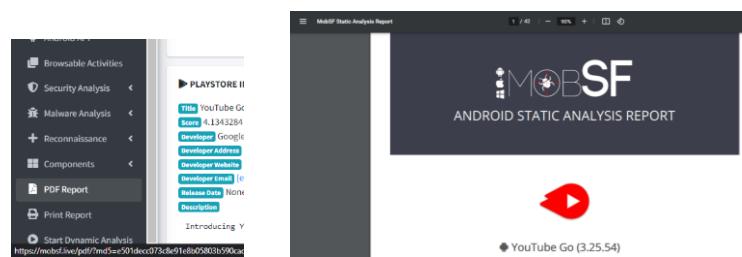
- Step 4:- Select any one android app and click open



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



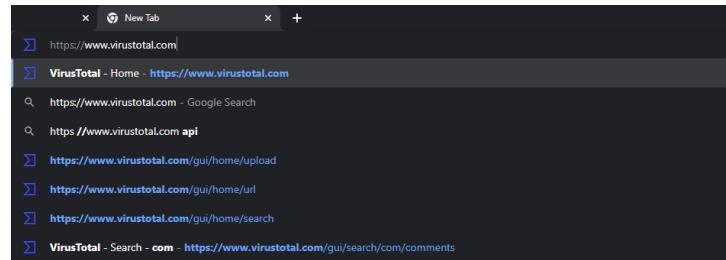
- Step 6:- after complet the analyse click on pdf report and save the report and analyse the report



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

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

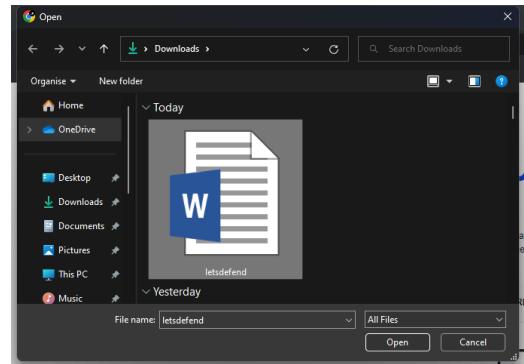
- Step 1:- Go to any browser and search <https://www.virustotal.com>



- 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



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE URL SEARCH



www.instagram.in

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your sample submission with the security community. Please do not submit any personal information. VirusTotal is not responsible for the contents of your submission. [Learn more](#).

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



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE URL SEARCH

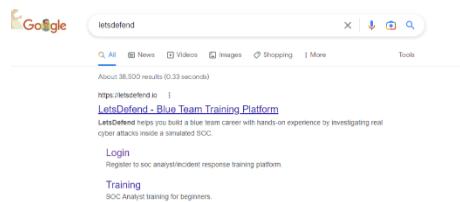


35.186.238.101

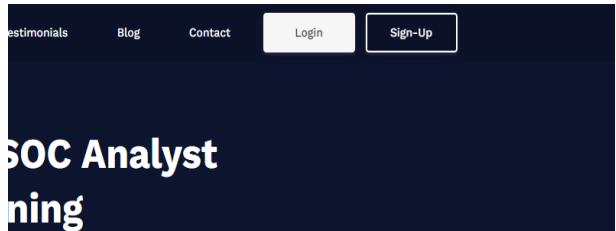
By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your sample submission with the security community. Please do not submit any personal information. VirusTotal is not responsible for the contents of your submission. [Learn more](#).

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

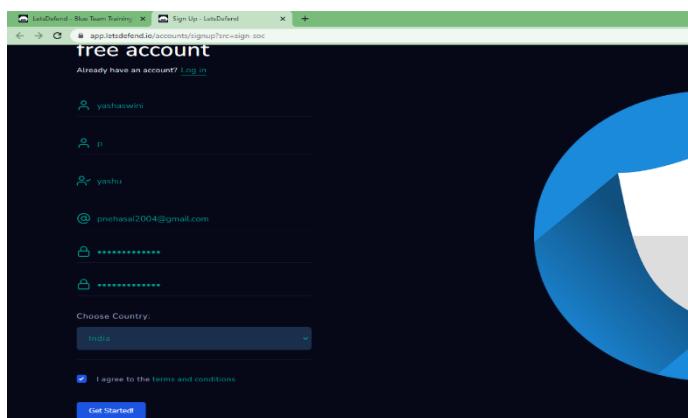
- **Step 1:** open google chrome and search for letsdefend



- **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

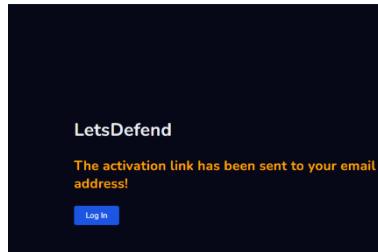
yashaswini, would you like to participate in our survey while waiting for the activation mail?

• Takes 30 sec/Windows
Go to Settings to activate Windows.
Start

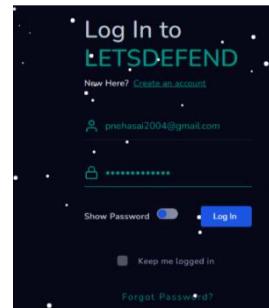
- **Step 5:** choose an answers for the given questions

| | | |
|---|--|--|
| <p>1. How did you discover LetsDefend? *</p> <p><input type="checkbox"/> A Search engine (Google, Yahoo, etc.) <input type="checkbox"/> B Recommended by friend or colleague <input type="checkbox"/> C Social media <input type="checkbox"/> D Blog or publication <input checked="" type="checkbox"/> diploma syllabus ✓</p> <p>OK ✓</p> | <p>2. What is your current role/level? *</p> <p><input checked="" type="checkbox"/> A Student ✓ <input type="checkbox"/> B SOC Analyst <input type="checkbox"/> C Manager / Team Leader <input type="checkbox"/> D C Level / Founder <input type="checkbox"/> E Security Engineer <input type="checkbox"/> F Other</p> <p>OK ✓</p> | <p>3. How much time do you spend improving your technical knowledge? *</p> <p><input checked="" type="checkbox"/> A Every day ✓ <input type="checkbox"/> B A few times a week <input type="checkbox"/> C A few times a month <input type="checkbox"/> D Other</p> |
| <p>4. What would you expect from a training platform? *</p> <p>You can choose 1 more</p> <p><input checked="" type="checkbox"/> A Quality contents ✓ <input type="checkbox"/> B Hands-on exercises <input type="checkbox"/> C Real world compatibility <input type="checkbox"/> D Ease of Use <input type="checkbox"/> E Lots of training material</p> <p>Submit</p> | | |

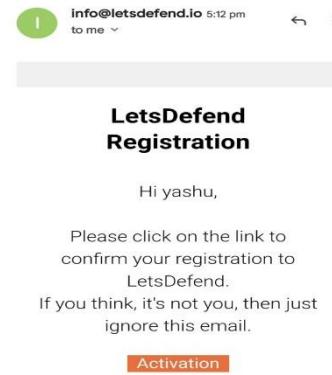
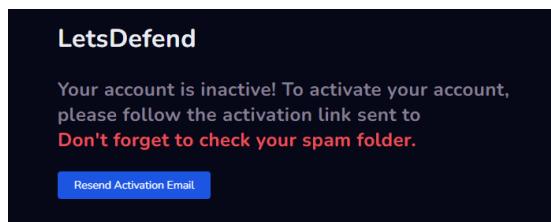
➤ **Step 6:** Click on log in



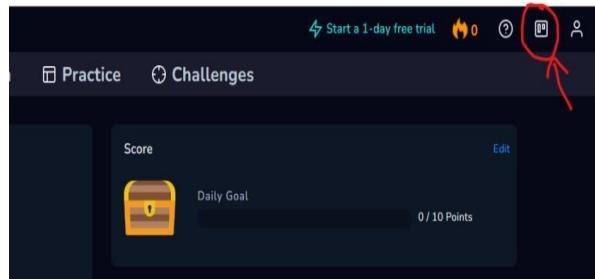
➤ **Step 7:** give an email and password for log in



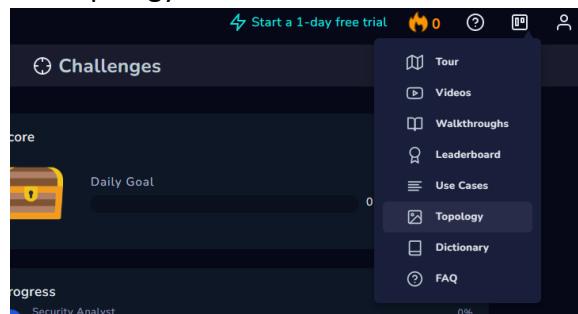
➤ **Step 8:** go to gmail in your mobile for activation and Click on Activation



➤ **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

