

Cyber Security Lab Manual

By
Gayathri D.Y,
Lecturer, Dept of CY

Table of Contents

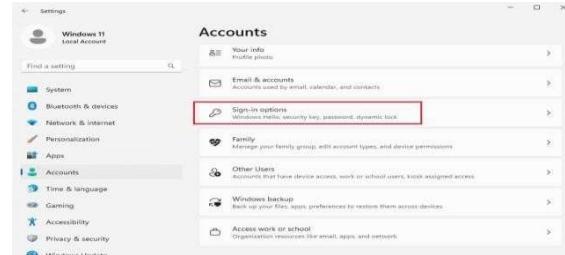
1. Change/set windows desktop security pin/ password, enable disable firewall & check windows update system	2
2. Demonstrate Turn on & off Windows OS Firewall.....	4
3. Check the browser and website certificates and analyze the certificates.....	5
4. Install Anti-virus and scan the computer.....	7
5. Install Git app and perform the basic git operations below.....	9
6. Design a simple crypto system [encryption, decryption, digital signature] using anycrypto tool	15
7. Crack a WIFI Password using wifite	21
8. Install VPN on mobile and pc and check connection.....	21
9. Demonstrate NTFS file system using NTFS permission reporter.....	23
10. Installation of process hacker and observe the process with all details.	26
11. Using the Microsoft threat model software, create a threat model for any applicationarchitecture.....	28
Create application.....	29
12. Install OWASP ZAP and demonstrate finding vulnerabilities in web application using automated scan & Manual Scan.	31
13. Create a cloud account in AWS & Access the IAM user service & create two user accounts & one group and add created users to the group and setup twofactor authentication to any one user.	33
14. Demonstrate the creation of S3 bucket service in AWS & store some files in S3bucket.....	39
15. Install the Apktool on your Virtual machine and perform reverse engineering on the DIVA Android application.	47
16. Download and install the android studio and create a AVD.....	49
17. Scan any 5 android apps and analyse the report's using MobSF.....	52
18. Using VIRUSTOTAL website Analyse any File, Url & Domain etc....	53
19. Give the procedure for Understanding the tools and products used in any organisation using letsdefend.io website	54

SIGNATURE OF COURSE CO-ORDINATOR

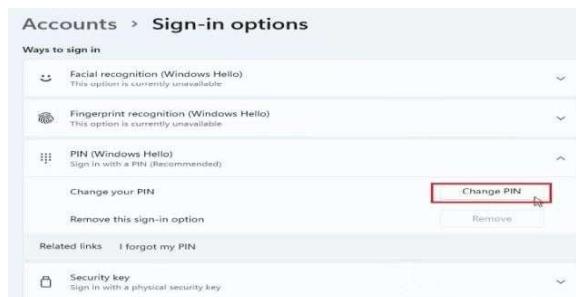
1. Change/set windows desktop security pin/ password, enable disable firewall & check windows update system

❖ **Password setup or change pin**

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



- 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.

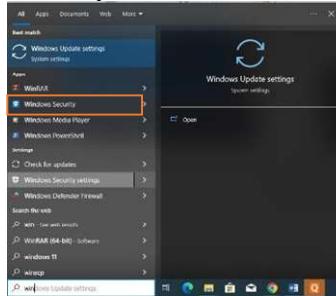


2. Demonstrate Turn on & off Windows OS Firewall

➤ Step 1: go to search



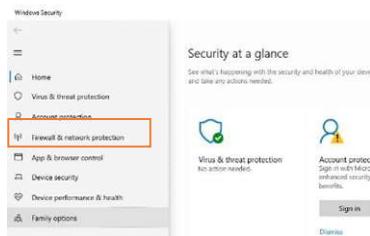
Step 2: search windows security



➤ 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 , nowyou can on & the firewall

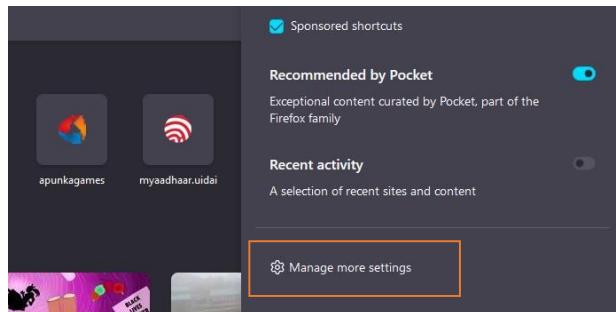


3. Check the browser and website certificates and analyze the certificates

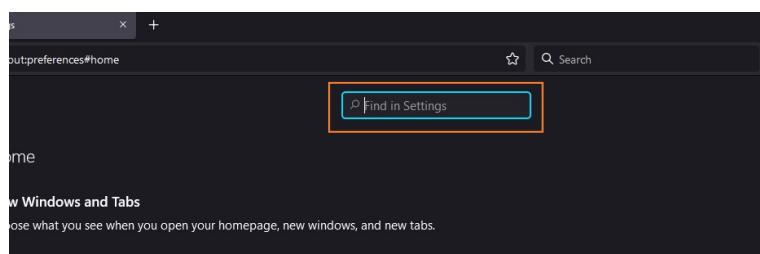
- ❖ Browser certificates view
- Step 1:- Open Firefox Browser and click on settings icon



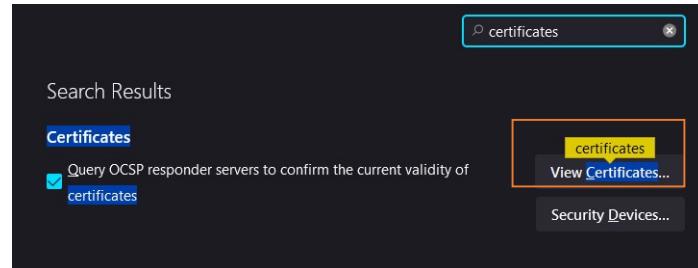
- Step 2:- click manage more setting option



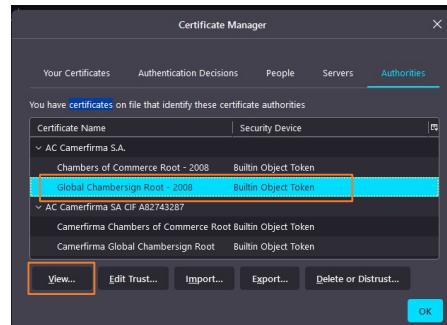
- Step 3:- Search certificates in search box



- Step 4:- Click on view certificates



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



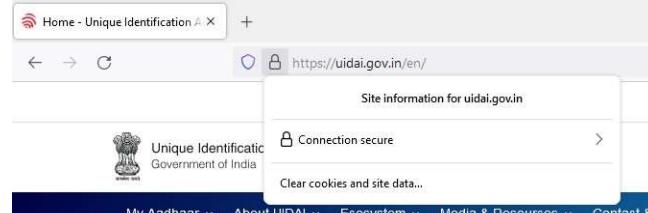
- Step 6:- Now you can see the certificate

Website certificate check

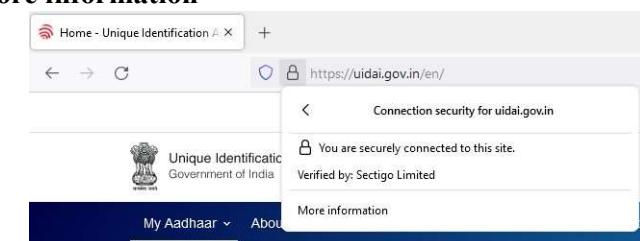
- Step 1:- Goto firefox and search any website
- Step 2:- Click lock icon on left side top corner



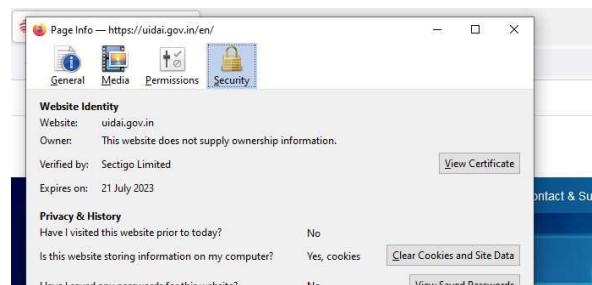
- Step 3:-Click connection secure



- 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

**Free antivirus is your first
step to online freedom**

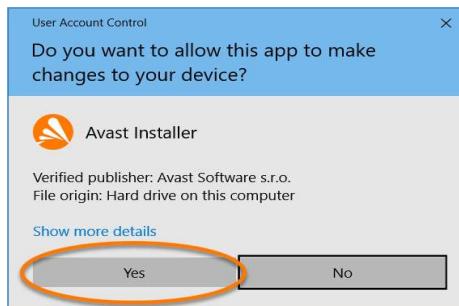
We believe everyone has the right to be safe online, which is why we offer our award-winning free antivirus to millions of people around the world.



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



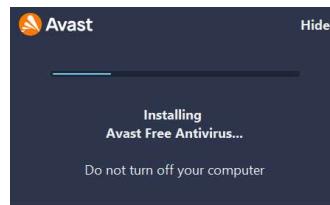
- Step 5: If prompted for permission by the User Account Control dialog, click Yes.



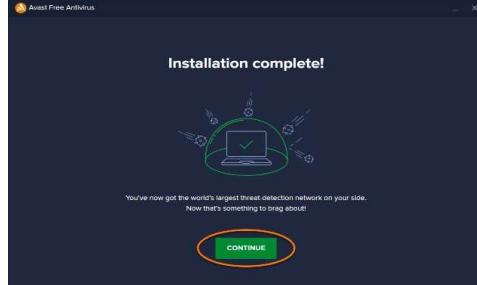
- Step 6: Then, click Install



- 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,



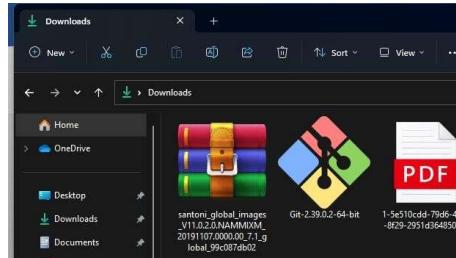
5. Install Git app and perform the basic git operations below

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

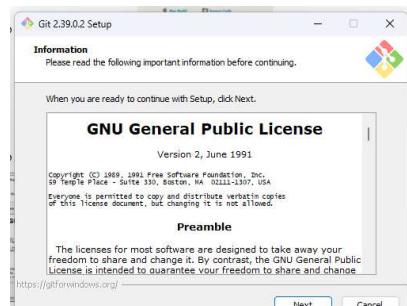
- Step 1: Browse to the official Git website: <https://git-scm.com/downloads>
- Step 2: Click the download link for Windows and allow the download to complete.



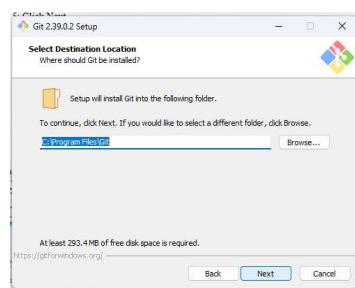
- Step 3: Double-click the file to extract and launch the installer.



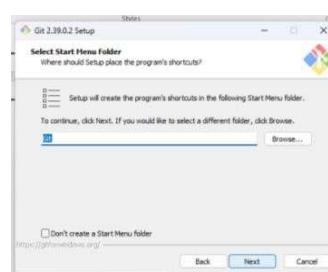
- Step 4: Click Next.



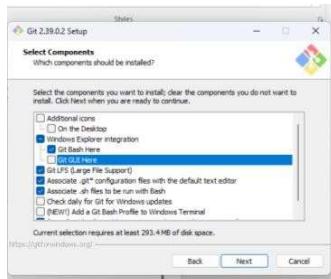
- Step 5: Click Next.



- Step 6: Click Next.



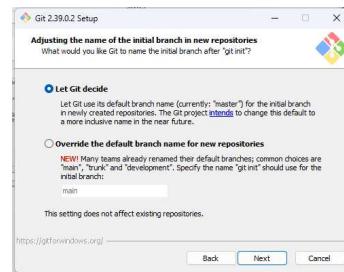
➤ Step 7: Simply click Next.



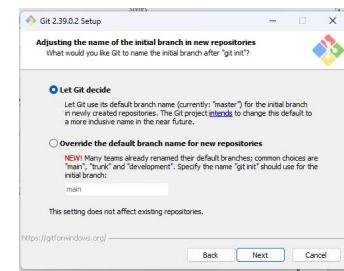
➤ Step 8: Click Next.



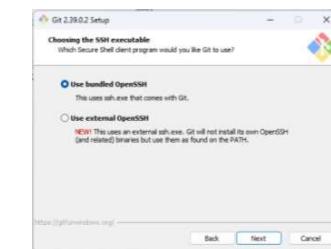
➤ Step 9: Click Next.



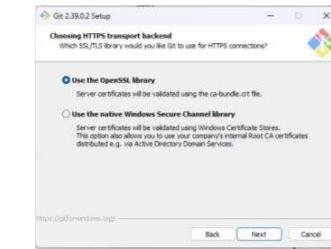
➤ Step 10: Click Next.



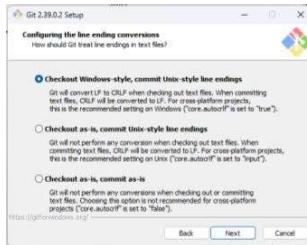
➤ Step 11: Click Next.



➤ Step 12: Click Next.



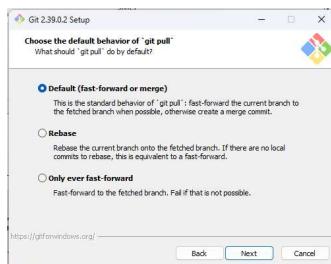
➤ Step 13: Click Next.



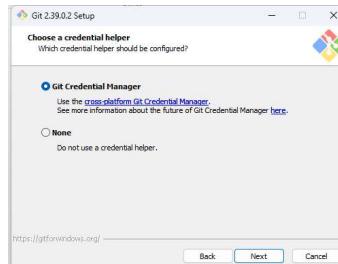
➤ Step 14: Click Next.



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



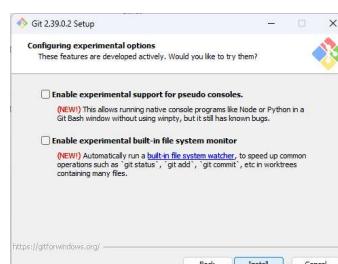
➤ Step 16: Click Next.



➤ Step 17: Click Next.



➤ Step 18: Click Install.



➤ Step 19: Click Finish.



basic git operations

- Create a folder **gitdemo** under “C:\Users\cse136”
- Cd “to repository path” → cd “C:\Users\cse136\gitdemo”
Here “gitdemo” is the repository”

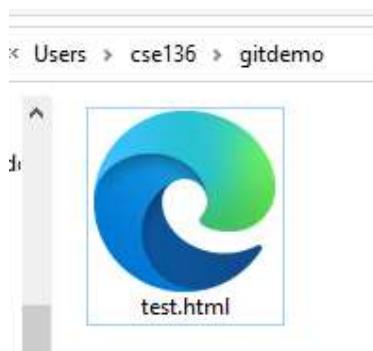
Now add username and email

- Git config --global user.name "user_name"
- Git config --global user.email "user_email id"
- Git status
- Git init

```
cse136@DESKTOP-8H3KNCS MINGW64 ~/gitdemo (master)
$ |
```

- touch test.html

Empty test.html is created



- Git commit -m create “test.html”

To save changes done in gitdemo repository

- Git status
- Git log

Write below html code in test.html

```
<html>
<head>
<title>test</title>
</head>
<body>
<h1>changes seen</h1>
</body>
</html>
```

test.html - Notepad

File Edit Format View Help

```
<html>
<head>
<title>test</title>
</head>
<body>
<h1>changes seen</h1>
</body>
</html>
```

Now save test.html

- **git status**

```
$ git status
On branch master
Changes to be committed:
  (use "git restore --staged <file>..." to unstage)
    modified:   test.html

Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
    modified:   test.html
```

- **git restore “test.html”**

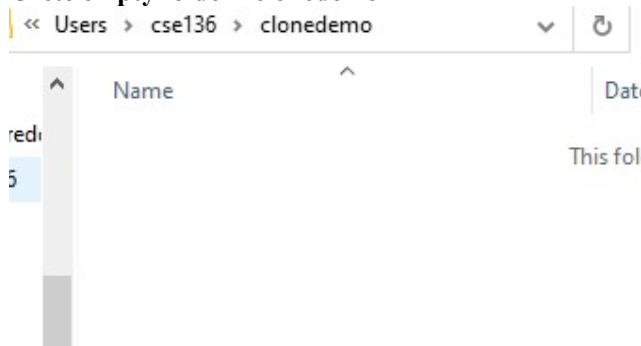
We can observe the data written in test.html is gone. File is reverted to its original state i.e test.html is empty

***test.html - Notepad**

File Edit Format View Help

Cloning repository

Create empty folder “clonedemo”



Open Git bash

Cd “file path to where repository must be clone” → clonedemo

Cd “C:\Users\cse136\clonedemo”

The screenshot shows a GitHub repository named '-cybersecurity' owned by 'sindhenvijju'. The repository has 1 branch and 0 tags. The README.md file contains an initial commit. On the right, there is a 'Clone' section with an 'HTTPS' link highlighted with a yellow box and a red circle around the copy icon.

Git clone “path from git website”

```
cse136@DESKTOP-8H3KNCS MINGW64 ~/gitdemo (master)
$ git clone "https://github.com/sindhenvijju/-cybersecurity.git"
Cloning into '-cybersecurity'...
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 4 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (4/4), 4.50 KiB | 148.00 KiB/s, done.

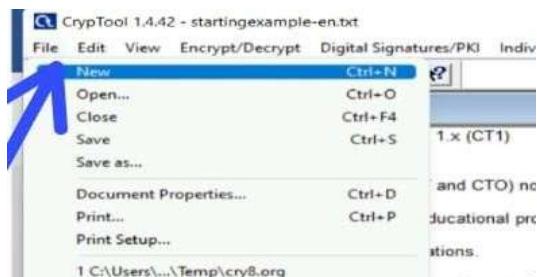
cse136@DESKTOP-8H3KNCS MINGW64 ~/gitdemo (master)
$ |
```

Browse to clone demo folder. Now we can see “cybersecurity” repository has been successfully cloned

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



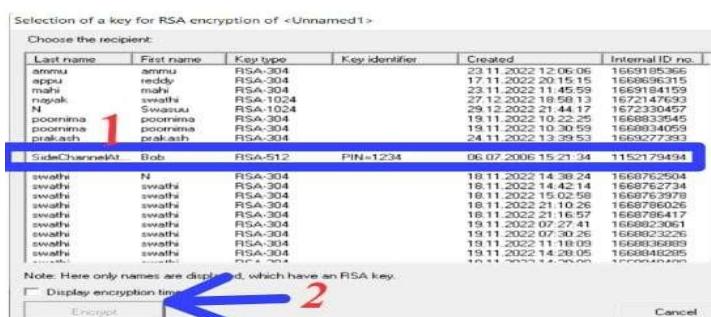
➤ Step 2: - Then type the message



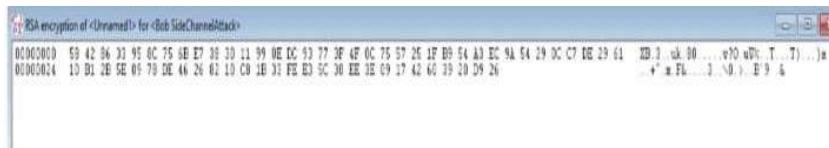
Step 3: - Go to Encryption/Decryption option & Select asymmetric Then Click on the RSA encryption



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

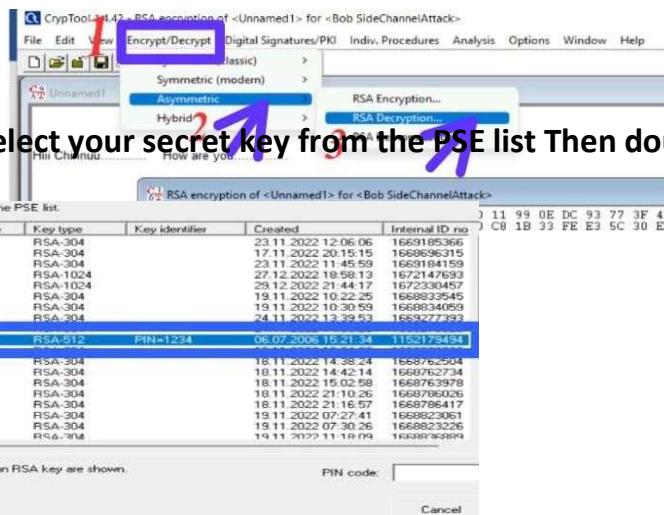


➤ Step 5: - Then your message will be encrypted

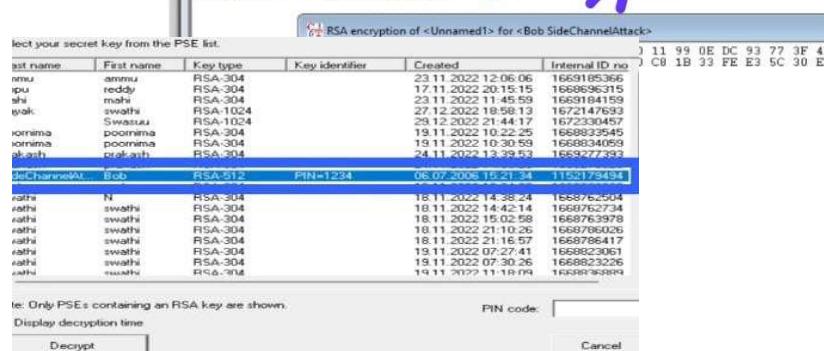


Steps for Decryption

Step 1: - Go to Encryption/Decryption & Select the asymmetric Then click on the RSAdecryption



➤ 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



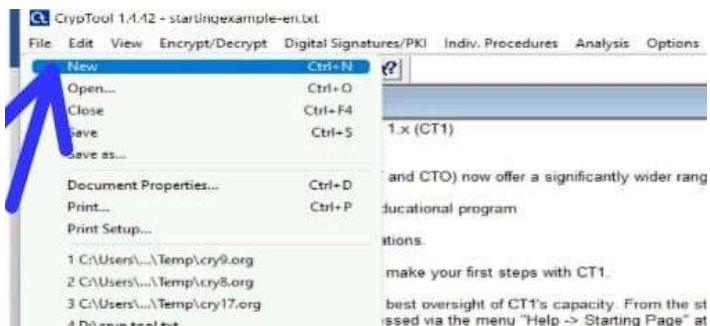
➤ Step 5: - Then your message will be decrypted



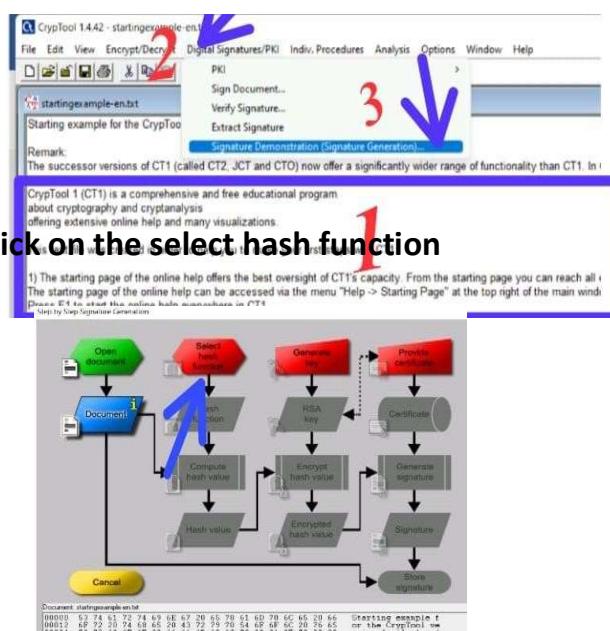
2E 2E 2E 2E 2E 2E 20 20 20 20 48 6F Hiii Chinnuu..... Ho
0A 00 00 w are you.....

Steps for Digital Signature

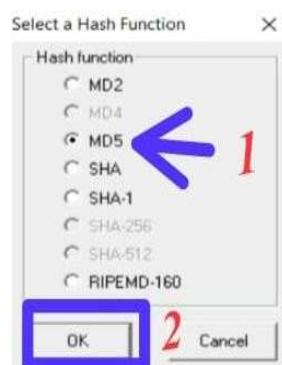
- Step 1: - Go to file Then click on the new



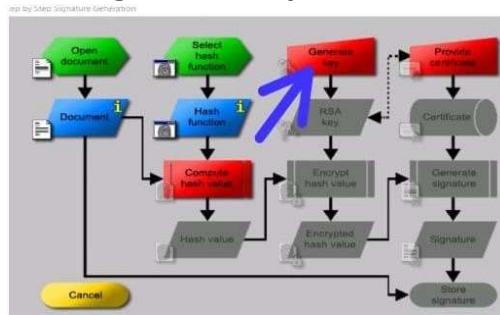
- Step 2: - Type the message & go to digital signature Then click on the signaturedemonstration



- 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 entity	<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"/>	
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)
- Generating all primes within the value range set for p

Separator for the display of the primes: []

Algorithms for prime number generation:

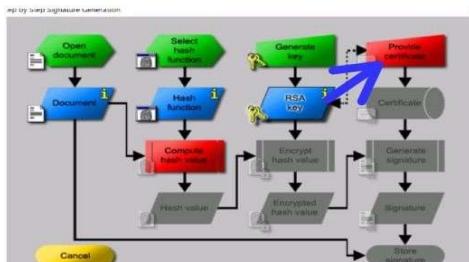
- Miller-Rabin Test
- Solovay-Strassen Test
- Fermat Test

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 <input type="text"/> 2^{150}	Upper limit <input type="text"/> 2^{151}
	Result <input type="text"/> 423163384625737737	
Prime number q	Lower limit <input type="text"/> 2^{150}	Upper limit <input type="text"/> 2^{151}
	Result <input type="text"/> 1434298724673852070	
<input type="button" value="Generate prime numbers"/> <input type="button" value="Apply primes"/> <input type="button" value="Cancel"/>		

➤ 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: 34755401522451565756725956555411746681920980041133310779009
- Public key e: 65537

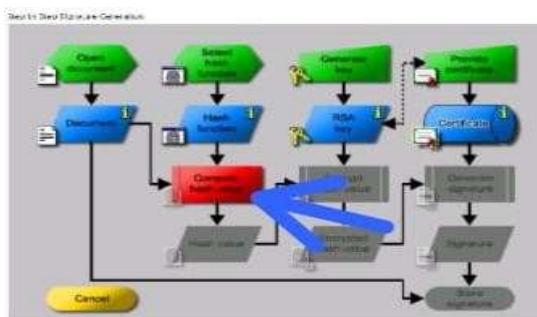
Personal data for the certificate:

Name: <input type="text"/> Swasuu	(optional)
First name: <input type="text"/> reddy	1
Key identifier: <input type="text"/>	
PIN: <input type="text"/>	
PIN verification: <input type="text"/>	

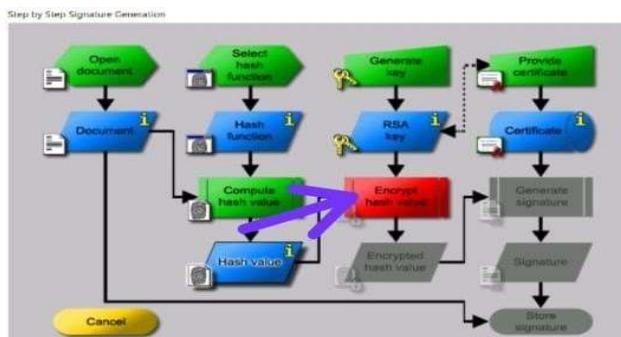
Generated names for PSE and certificate:

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

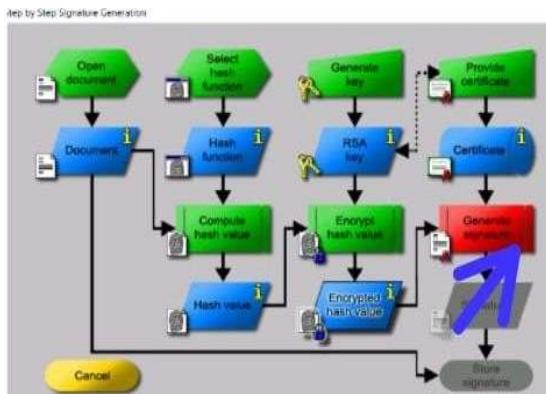
➤ Step 11: - Then click on the compute hash value



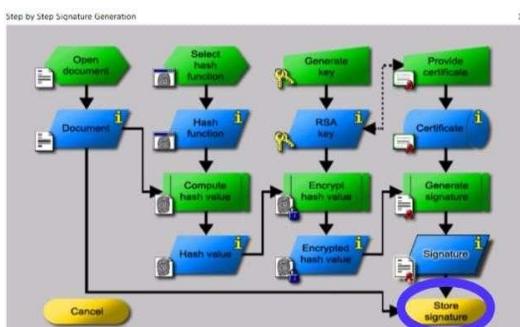
➤ Step 12: - Click on the encrypt hash value



➤ Step 13: - Then click on the generate signature



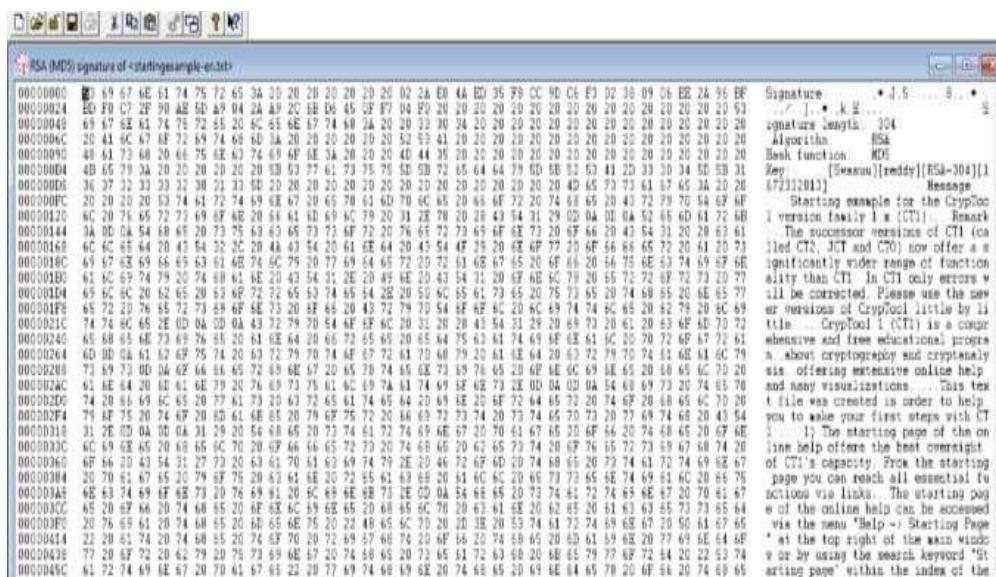
➤ Step 14: - Click on the store signature



➤ 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

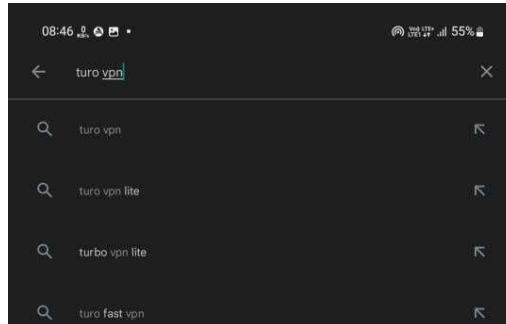
```
[+] select target(s) (1-4) separated by commas, dashes or all: 1
[+] (1/1) Starting attacks against 94:6A:B0:15:41:6A (hug2g858469)
[!] Skipping PMKID attack, missing required tools: hcxdumptool, hcxpcaptool
```

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

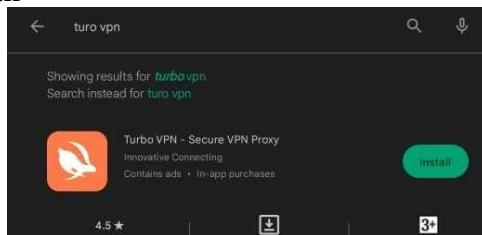
8. Install VPN on mobile and pc and check connection.

❖ On Mobile

- step 1:-open Playstore and search turbo vpn



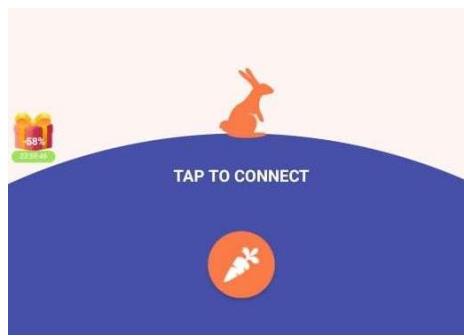
- ## ➤ Step 2:- click install



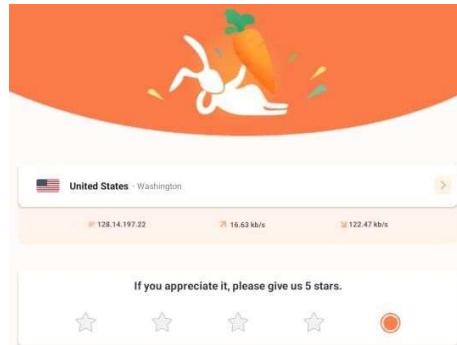
- Step 3:-open turbo vpn and click agree & continu



- #### ➤ Step 4:- press tap to connect



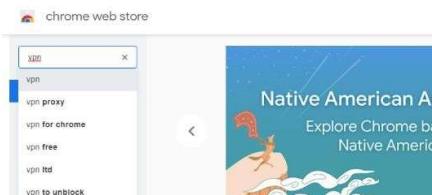
- Step 5:- vpn connected successfully



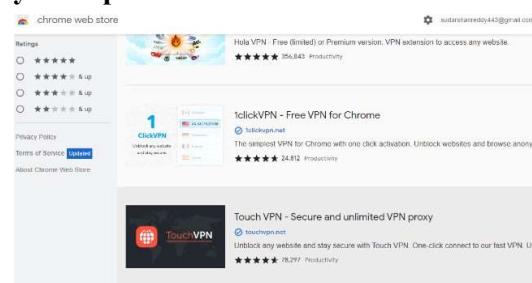
- On Computer
- Step 1:- open chrome browser and search “<https://chrome.google.com/webstore>”



- Step 2:- search vpn on webstore



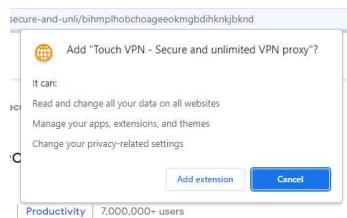
- Step 3:- Click any one vpn



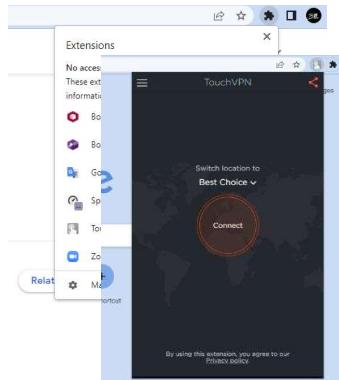
- Step 4:- click add to chrome button to install vpn



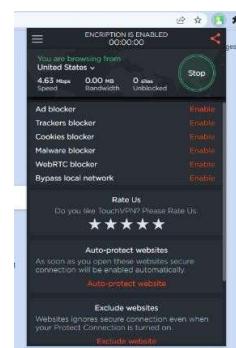
- Step 5:- Click add extension to confirm



- 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.permissionreporter.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-related 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 proven user friendly tool for reporting on directory permissions on your Windows file servers. It lets you quickly see which ...

<https://blog.renix.com/infrastructure>
Top 11 NTFS Permissions Tools for Smarter Administration
 13-Jan-2021 – 1. NTFS Permissions Reporter Free Edition from Cjdev - 2. Netwrix Effective Permissions Reporting Tool - 3. Microsoft's AccessEnum - 4.

- Step 2: Click on Download Now



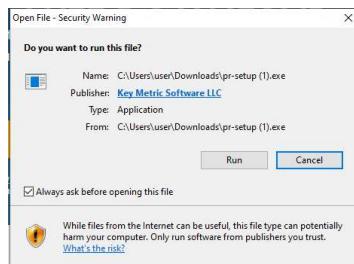
THE NTFS PERMISSIONS ANALYZER FOR WINDOWS

Activate Windows

➤ Step 3: Click on Start Download

The screenshot shows the PermissionsReporter website's download page. At the top, there's a navigation bar with links for Home, Screens, Features, Download (which is underlined), Order, and Support. Below the navigation is a large blue banner with the text "FREE DOWNLOAD" and a "Start Download" button. A small note says "Just click the button below to download, then install on any supported computer." To the right of the download button is a preview image of the software's interface, labeled "FREE BASIC EDITION". Below the banner, there's a section titled "PERMISSIONS REPORTER REQUIREMENTS" with a note: "Any 64-bit Edition of Windows 11, 10, 8.1, 7 (SP1) or Windows Server 2022, 2019, 2016, 2012." At the bottom of the page, there are two buttons: "BUILT FOR 64 BIT" and "PRODUCT HELP".

➤ Step 4: Click Run



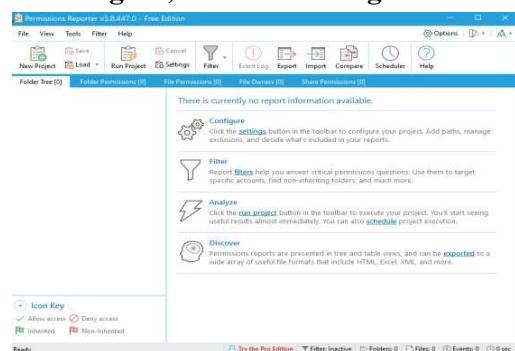
➤ Step 5: Click on Next



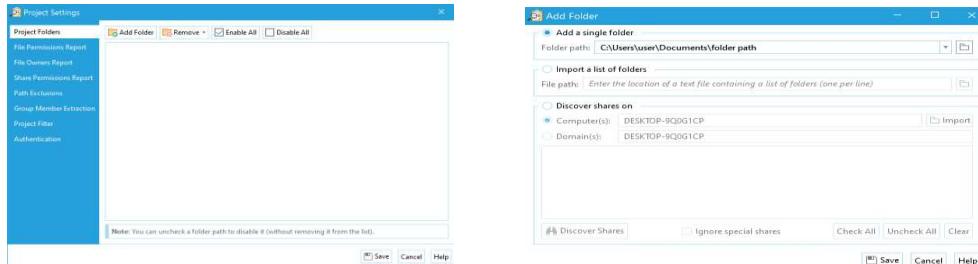
➤ Step 6: Click on Close



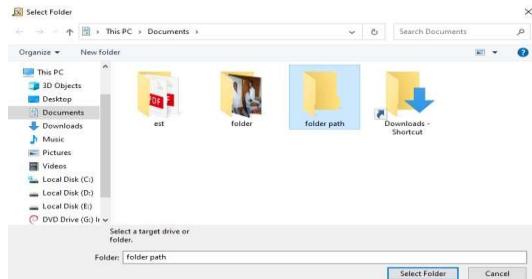
- Step 7: open the permission reporter
- Step 8: In Configure, Click on settings



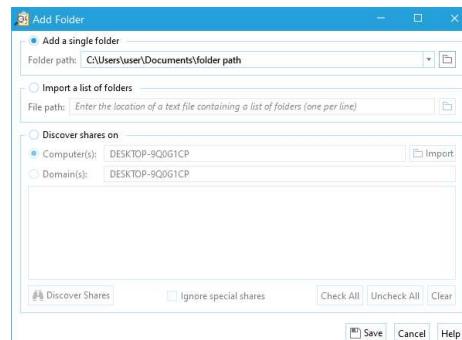
➤ Step 9: In project settings, Select Add Folder



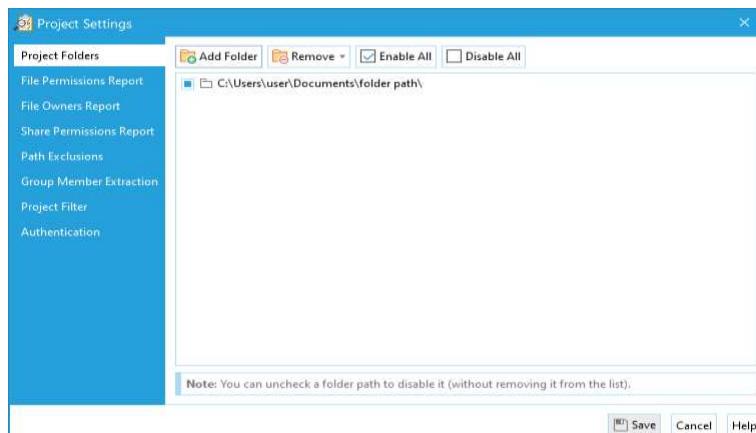
➤ Step 10: Select the folder and Click on Select Folder



➤ Step 11: Click on Save



➤ Step 12: Click on Save



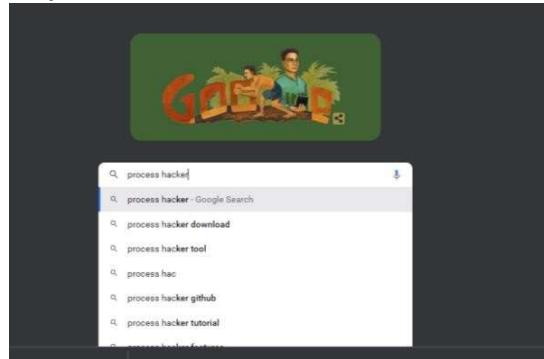
➤ Step 13: Click on the run project

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

Type	Inherited	Account	Basic Permissions	Scope
Allow		BUILTIN\Administrators	Full control	This folder, subfolders, and files
Allow		NT AUTHORITY\SYSTEM	Full control	This folder, subfolders, and files
Allow		DESKTOP-9QDG1CP\user	Full control	This folder, subfolders, and files

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

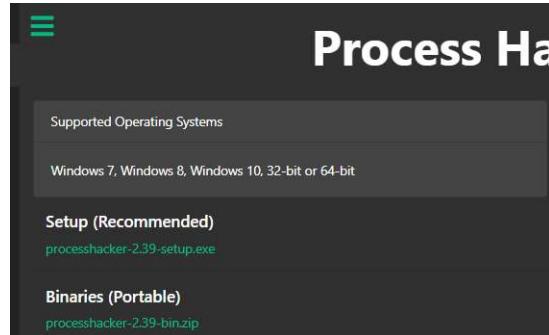
- Step 1: - Go to any browser & Search Process Hacker



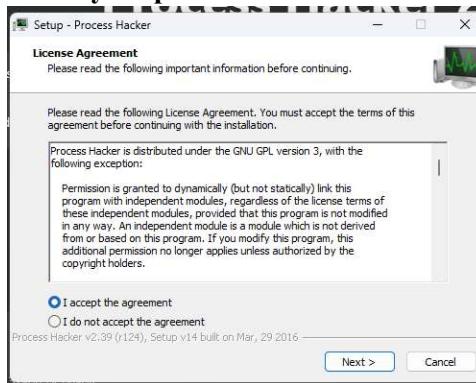
- Step 2: - Search the download process hacker



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



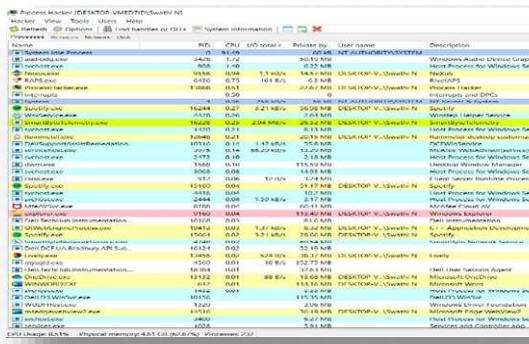
- Step 4: - Process hacker will be downloaded
- Step 5: - Then process hacker will be displayed on the screen
- Step 6: - Double click on the process hacker
- Step 7: - Then click on yes option and click on the next



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

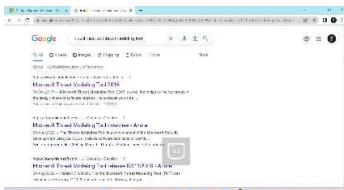


- Step 10: - Then you can observe the process with all details



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

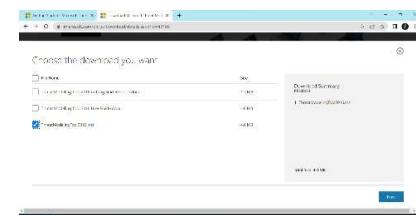
- Step 1 go to any browser search Microsoft threat Modeling tool download



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



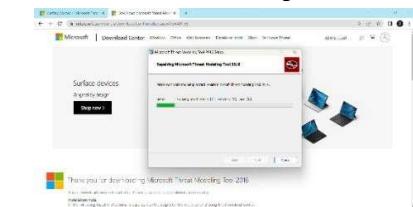
- Step 3 Choose the download you want ThreatModelingTool2016.msi 4.0 click Next



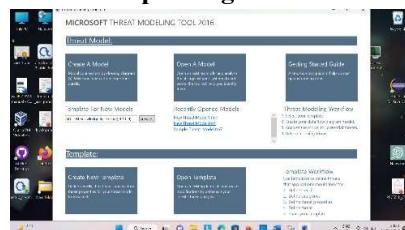
- Step 4 Click Next



- Step 5 finish the installation click next step

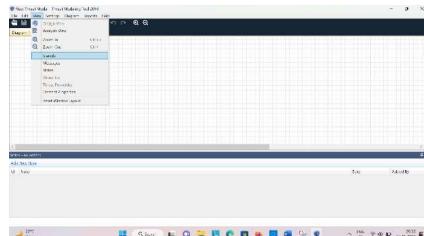


- Step 6 After installation completed go to Threat Model create A Model

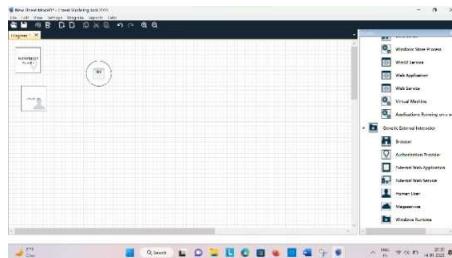


Create application

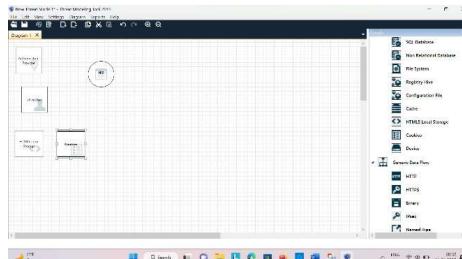
- Step 7 go to view click stencils display the tools



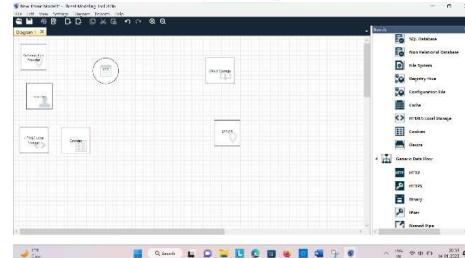
- Step 8 Take application, Human user, Authentication provider and give the permission



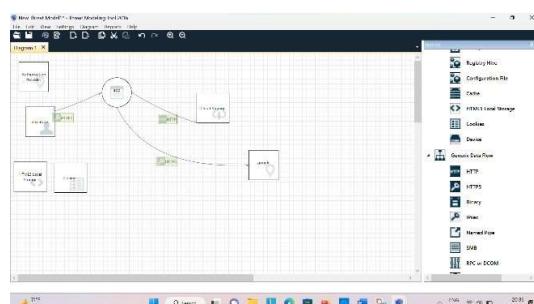
- Step 9 Take local storage HTML and security cookies



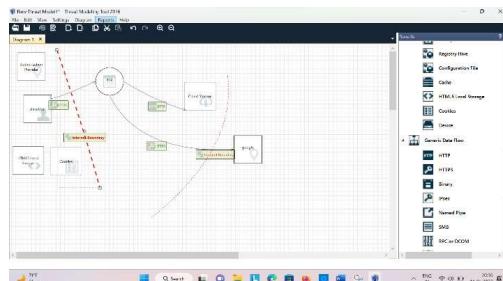
- Step 10 Take browser and cloud storage give a permission



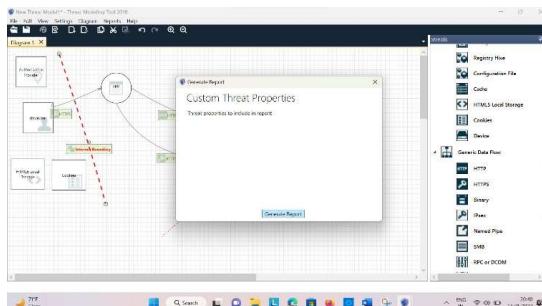
- Step 11 Assign HTTPS user, google to app and HTTP app to storage



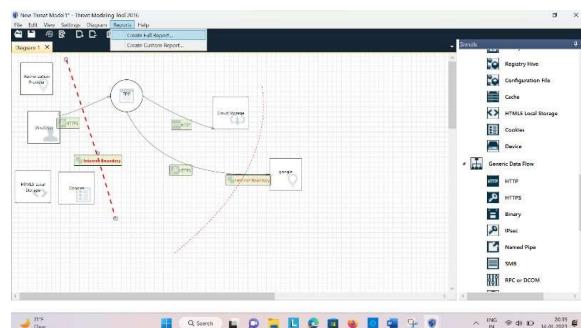
➤ **Step 12 Add Internet Boundary and got reports**



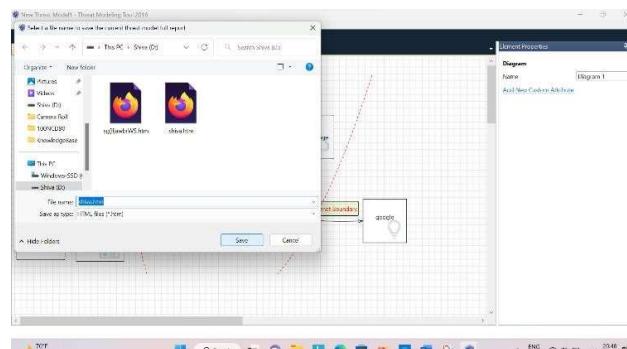
➤ **Step 13 Click Create Full Report**



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



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

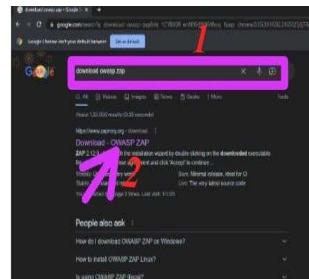


➤ **Step 16 Report will be generated find the vulnerability and threat in your application**

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

* Automated scan:

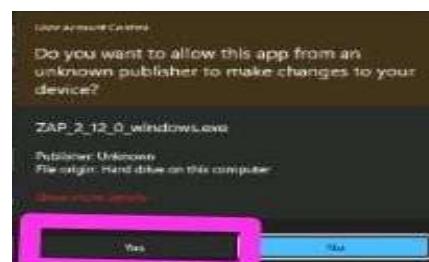
- Step 1: - Go to chrome & search the download OWASP ZAP then click on the download – OWASP ZAP



- 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

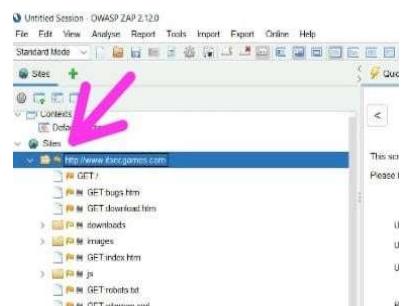


- Step 6: - Open the OWASP ZAP then click on the Automated scan

- 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 comeBack 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 twofactor authentication to any one user.

- Step 1: - Open the chrome browser & search the AWS then click on theamazon 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

The screenshot shows the 'Sign up for AWS' page. It has fields for 'Root user email address' (swasuureddy143@gmail.com) and 'AWS account name' (swasu). A large orange 'Verify email address' button is at the bottom.

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

The screenshot shows the 'Sign up for AWS' page under 'Confirm you are you'. It includes a 'Verification code' field containing '102895', a 'Verify' button, and a 'Resend code' button. Below the code field is a note about getting the code.

➤ Step 5: - Enter Root user password & confirm the password then

click on Continue

The screenshot shows the 'Sign up for AWS' page under 'Create your password'. It has fields for 'Root user password' and 'Confirm root user password', both with masked input. A green success message box says 'It's you! Your email address has been successfully verified.' Below the fields is a note about the importance of the password.

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

The screenshot shows the 'Sign up for AWS' page under 'Who should we contact about this account?'. It contains fields for '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), and 'Postal Code' (562101). A note at the bottom states that Indian contact addresses are served by Amazon Web Services India Private Limited, the local seller for AWS services in India. A checkbox for 'I have read and agree to the terms of the AWS Customer Agreement' is checked.

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

Credit or Debit card number:

AVS accepts all major credit and debit cards. To learn more about payment systems, review our FAQs.

Expiration date: October 2026

Cardholder's name: N PAVITHRA

CVN:

Billing address:

Use my contact address:
Bharat Cotton market road vijaynagar 1st floor
chikkalallapur karnataka 562101
IN

Use a new address:

Do you have a PAN? Permanent Account Number (PAN) is a ten-digit alphanumeric code issued by the Central Board of Direct Taxes Department. This 10-digit number is printed on the front of your PAN card.

Yes

No

Please go to 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: 4000 0000 0000 7433

Authenticate Payment
We have sent an OTP to your mobile number 8880000006

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: 45mhf2

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.

<input checked="" type="radio"/> Basic support - Free • Recommended for individual users and small teams • 24x7 self-service access to AWS resources • Free support and billing issues only • Access to AWS Health Dashboard & Trusted Advisor	<input type="radio"/> Developer support - From \$29/month • Individual developer support • Development and testing with AWS services • Email access to AWS Support • Business Hours • 24x7 support for minor responsive issues	<input type="radio"/> Business support - From \$100/month • Individual developer support • Running production workloads • 24x7 support for critical AWS services • 1-hour response time • Full set of Trusted Advisor recommendations
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Need Enterprise level support?

From \$16,000 a month you will receive 15-minute response times and concierge-style assistance with an assigned Technical Account Manager. Learn more

Complete sign up

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



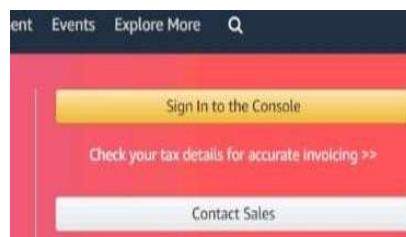
Congratulations

Thank you for signing up for AWS.

It's your account, which should only take a few minutes. You will receive this is complete.

Go to the 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

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
swasuureddy143@gmail.com

Next

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

Type the characters seen in the image below

syfr6

Submit

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

Root user sign in

Email: swasuureddy143@gmail.com

Password [Forgot password?](#)

Sign in

- Step 17: - Then click on IAM

- Step 18: - Click on user

No recently visited services

Explore one of these commonly visited AWS services:

IAM EC2 S3 RDS Lambda

Access management

- User groups
- Roles
- Policies
- Identity providers
- Account settings

Access reports

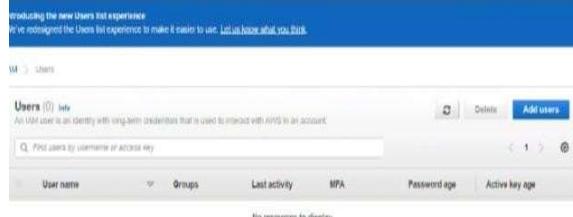
- Access analyzer
- Archived rules
- Analyses

Root user has no active access keys

IAM resources

User groups	Users	Roles
0	0	2

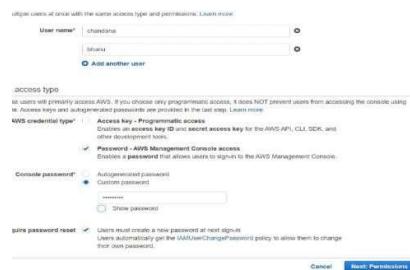
➤ Step 19: - Then click on Add user



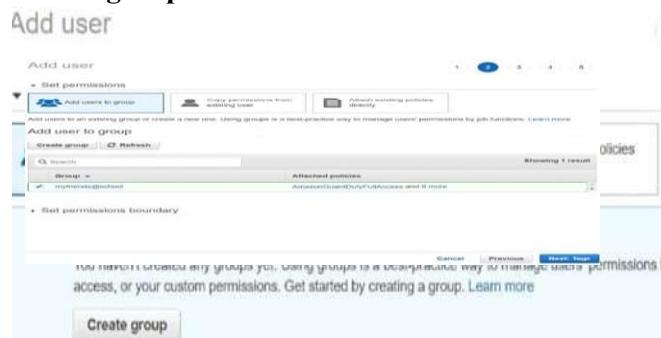
➤ Step 20: - Enter user name then if you want add multiple user

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

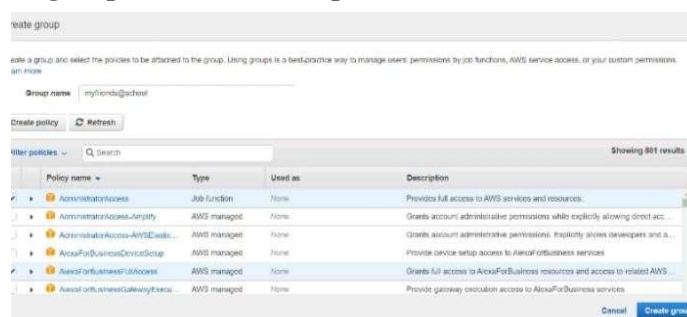
Select the password – AWS MCA. then Select the customer password& Enter the password. Then click on Next: permission



➤ Step 21: - Click on create group

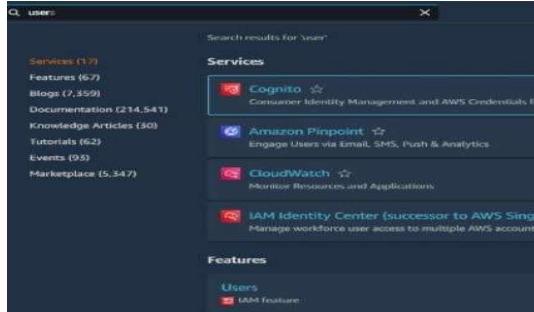


➤ Step 22: - Enter the group name & Give a policies then click on create group



➤ Step 23: - Then group will be created

➤ Step 24: - Search the users then click on users



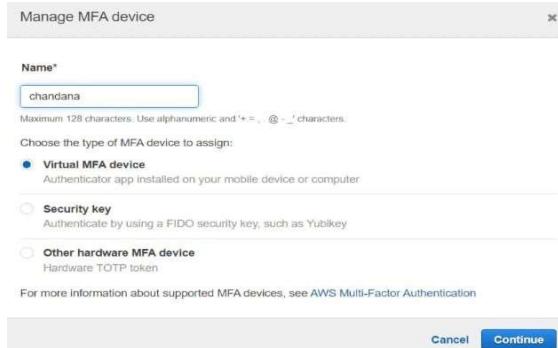
➤ Step 25: - Then click on Add MFA



➤ 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

theAuthenticator app



- Step 30: - Enter the numeric code from the authentication into the

AWSconsole. Then wait for a new code to appear in the authenticator.

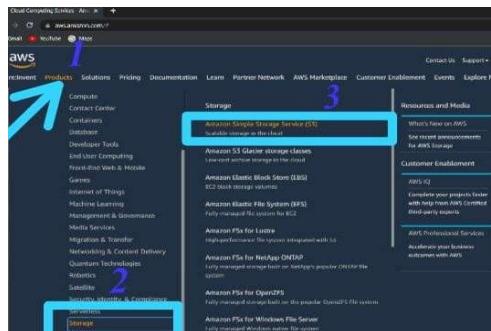
Enter the second code. Then click on “Assign MFA”



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

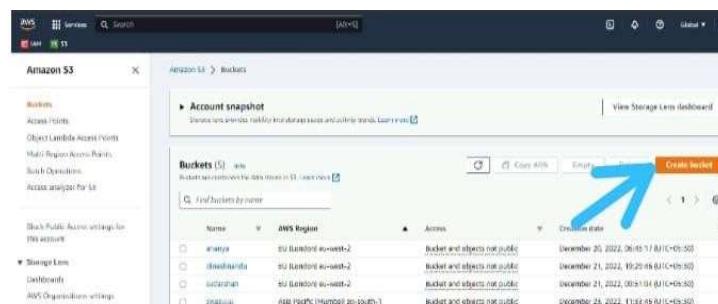
then click on the Amazon simple storage service(S3)



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



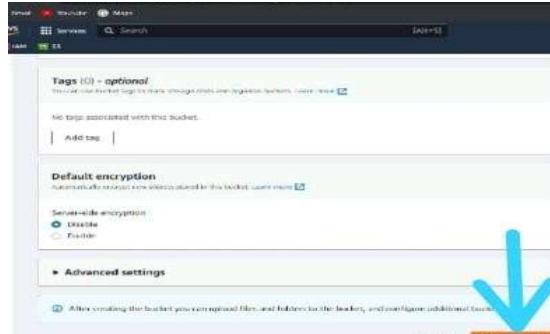
➤ Step 3: - Then click on create bucket



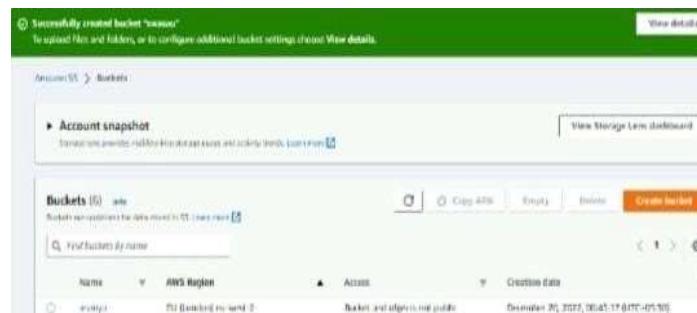
➤ Step 4: - Enter the bucket name then scroll down



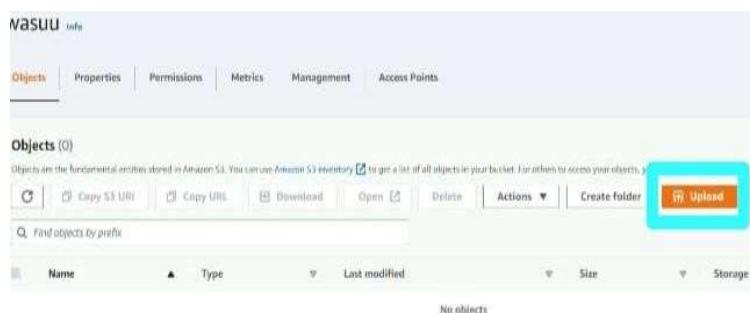
➤ Step 5: - Click on create bucket



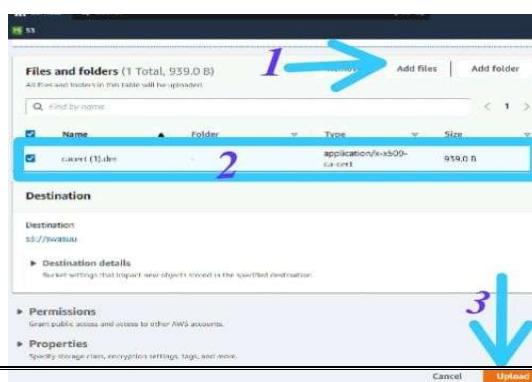
➤ Step 6: - Then bucket will be created



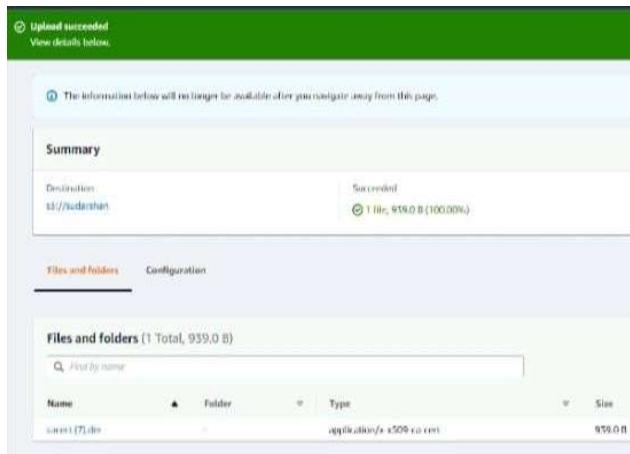
➤ Step 7: - Select the bucket then click on the upload option



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



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

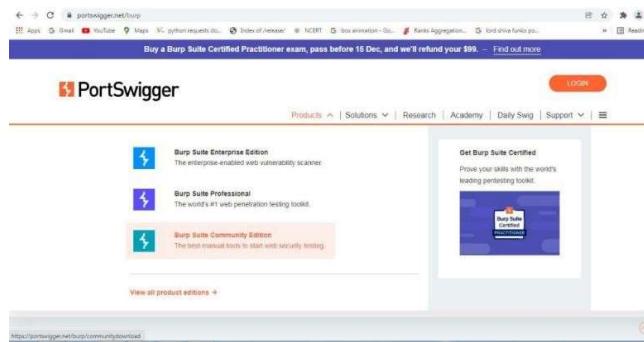


15. Installing Burp Suite on Windows & Import proxy server CA certificate to browser

- 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 CommunityEdition 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

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

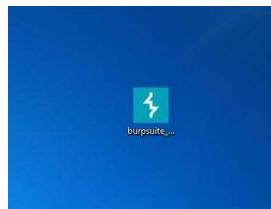
Professional / Community 2021.10.3

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)

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



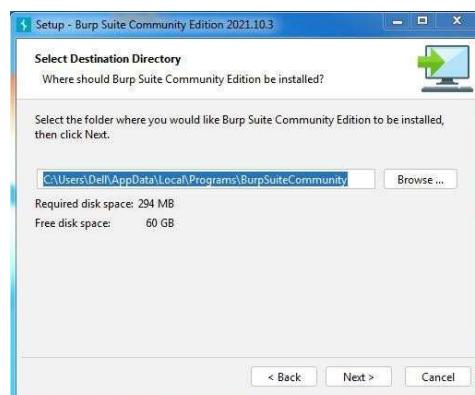
- Step 7: Loading of Installation Wizard will appear which will take a few seconds.



- 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.



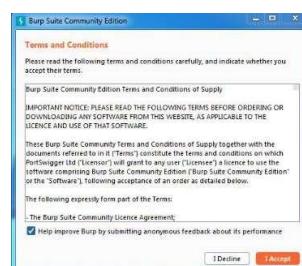
➤ Step 12: Click on Finish



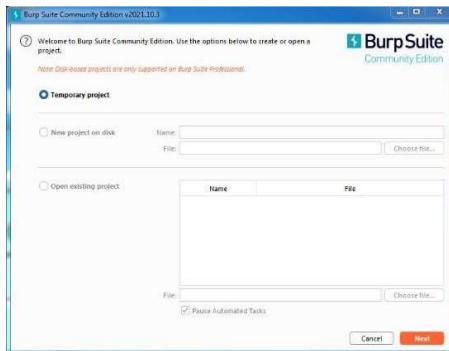
Step 13: Burp suite is successfully installed on the system and an icon is created on the desktop



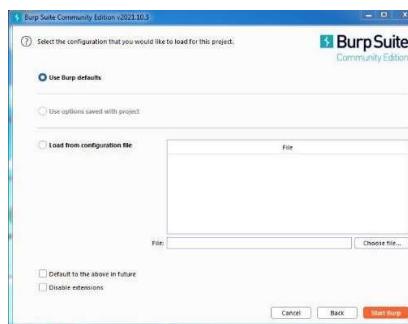
Step 14: Run the software, Click on I Accept.



➤ Step 15: Choose click Next.



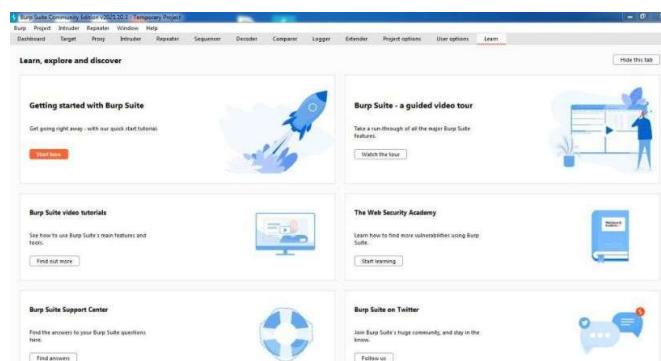
➤ Step 16: click on Use Burp Defaults.



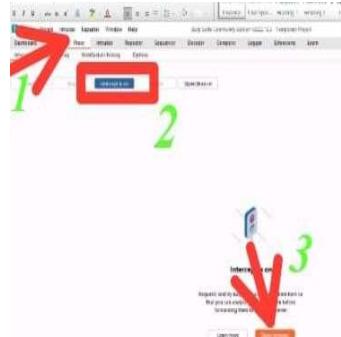
➤ Step 17: Project will start loading.



➤ 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 theStart burp
- Step 2: - Now burp suite will be open & select the proxy and turn on theIntercept then click on the open browser option



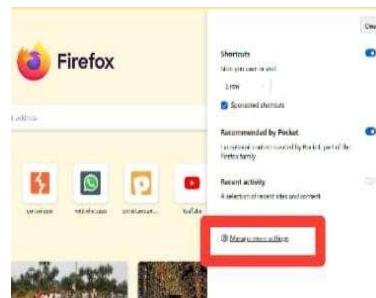
- Step 4: - Search the <http://Burpsuite> then click on the CA certificate
- Step 5: - Then CA certificate will be downloaded



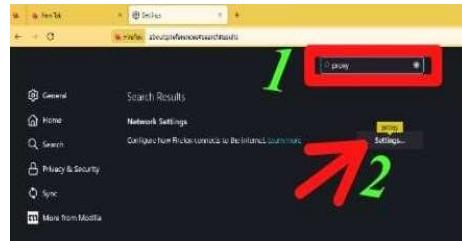
- Step 6: - Open the fire fox then go to settings



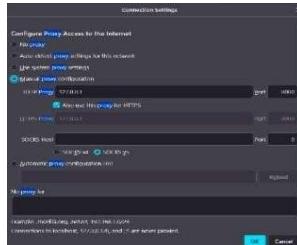
- Step 7: - Then click on the manage more settings



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



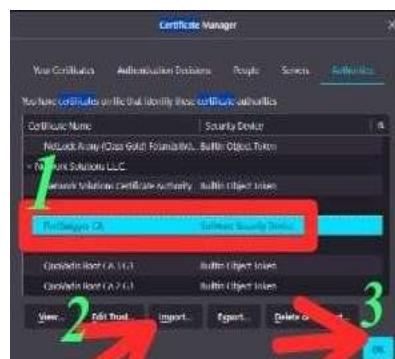
- Step 9: - Choose the manual proxy configuration & enter the HTTP proxy and Port then click on ok option EX: - 127.0.0.1 & 8080



- 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

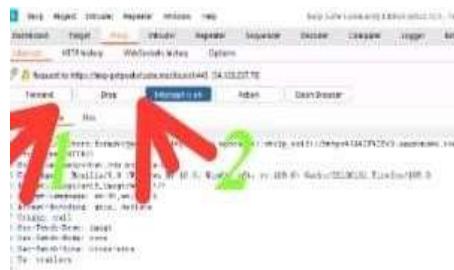


- Step 12: - Open the fire fox then search the any website name\

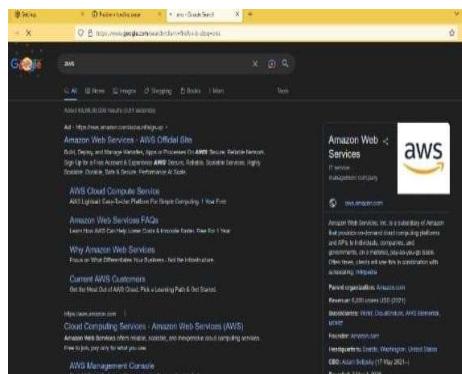
- Step 13: - Now we can't reach the website, So



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



- Step 15: - Now we can reach the website



15. Install the Apktool on your Virtual machine and perform reverse engineering on the DIVA Androidapplication.

- 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>

```
[kali㉿kali]: ~]$ git clone https://github.com/xAltMime/diva-apk-file.git  
Cloning into 'dipa-apk-file'...  
remote: Enumerating objects: 14, done.  
remote: Counting objects: 100% (14/14), done.  
remote: Compressing objects: 100% (14/14), done.  
Receiving objects: 42% (6/14)
```

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

```
File Machine View Input Devices Help
[ kali@kali: ~ ] 1 2 3 4 [ kali@kali: ~/diva-apk-file ]
File Actions Edit View Help
[ kali@kali: ~ ] cd diva-apk-file
[ kali@kali: ~/diva-apk-file ]
[ kali@kali: ~/diva-apk-file ] ls
DivaApplication.apk LICENSE README.md
[ kali@kali: ~/diva-apk-file ]
[ kali@kali: ~/diva-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
Screenshot taken
View image

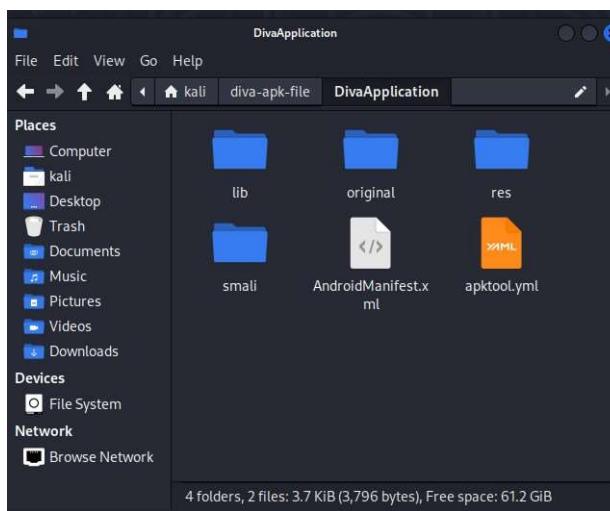
File Actions Edit View Help
-0,-output <dir> The name of folder that gets written. Default is apk.out
--frame-path <dir> User framework files located in <dir>.
-r,-no-res Do not decode resources.
-s,-no-src Do not decode sources.
-t,-frame-tag <tag> Uses framework files tagged by <tag>.
usage: apktool [build] [options] <apk_path>
-e,-efiles <apk> Clean extraction and build all files.
-o,-output <dir> The name of apk that gets written. Default is dist/name.apk
-p,-frame-path <dir> Uses framework files located in <dir>.

For additional info, see: https://ibotpeaches.github.io/Apktool/
For small/bad/small info, see: https://github.com/JesusFreke/small

[Kali㉿kali:~/diva-apk-file]
$ ls
DivaaApplication.apk LICENSE README.md

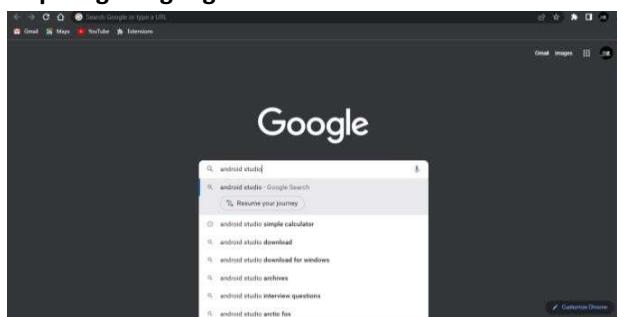
[Kali㉿kali:~/diva-apk-file]
$ apktool d DivaaApplication.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=true -Dswing.aatext=true
I: Using Apktool 2.6.1-irtyS on DivaaApplication.apk
I: Loading resource table from file: /home/kali/.local/share/apktool/framework/1.apk
I: Decoding AndroidManifest.xml with resources ...
I: Loading resource table from file: /home/kali/.local/share/apktool/framework/1.apk
I: Regular manifest package ...
I: Decoding file-references ...
I: Decoding assets ...
I: Decoding apk ...
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 sourcecode

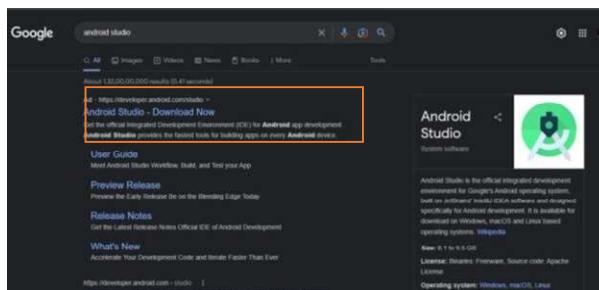


16. Download and install the android studio and create a AVD

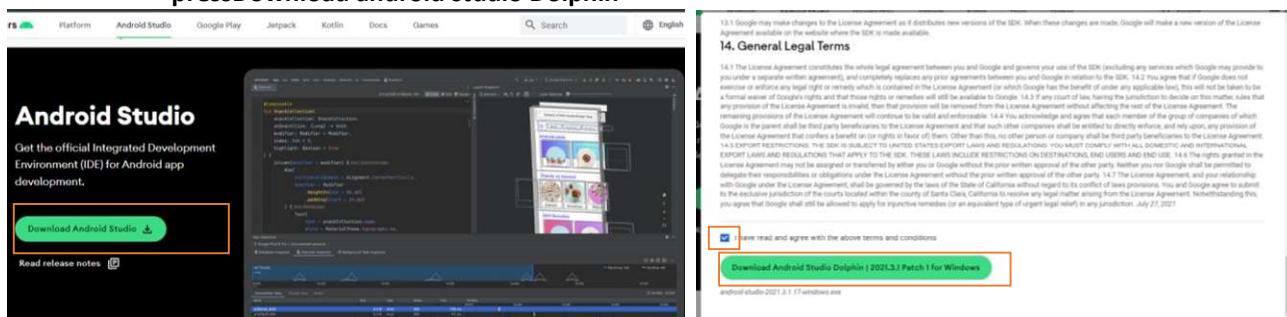
- Step 1:- go to google and search android studio



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



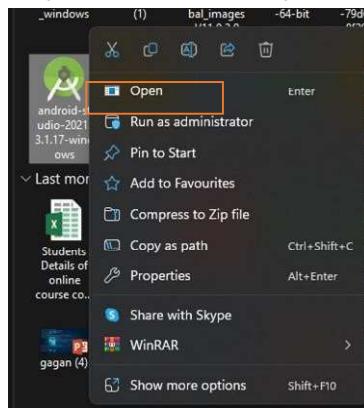
- Step 3:-Now click download android studio option & and click terms and conditions and pressDownload android studio Dolphin



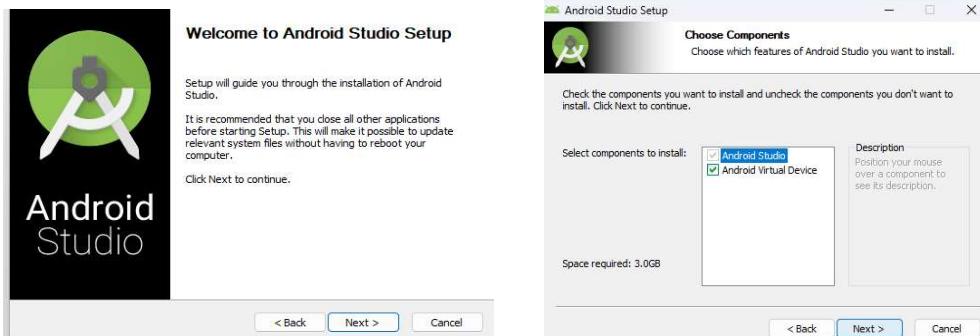
- Step 4:- Wait until download complet



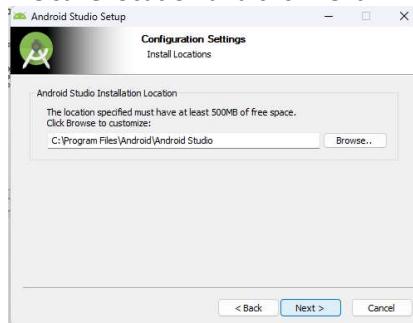
➤ Step 5:- After complet the download open the software



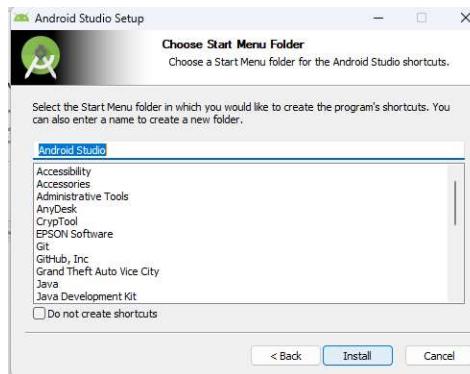
➤ Step 6:- Click next button and Choose Components and click next.



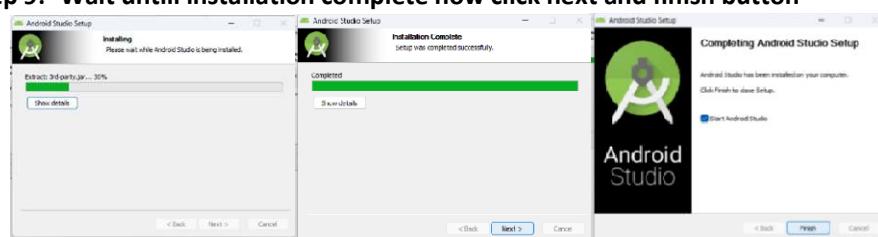
➤ Step 7:- Select File save location and click next.



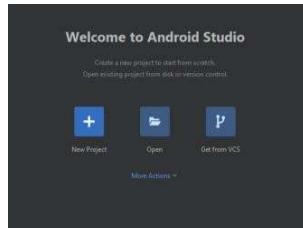
➤ Step 8:- select Installation Directory's and click install



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



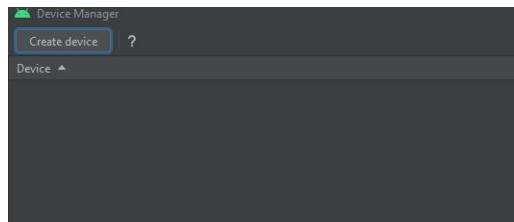
➤ Step 10:- Click on more Actions



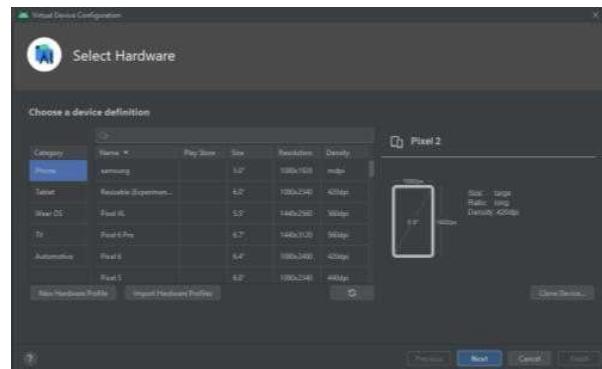
➤ Step 11:- Now click on Virtual Device Manager



➤ Step 12:- Click on create device



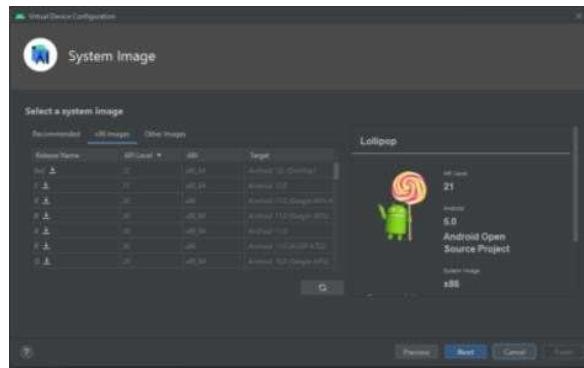
➤ Step 13:-select any one category & model then click next



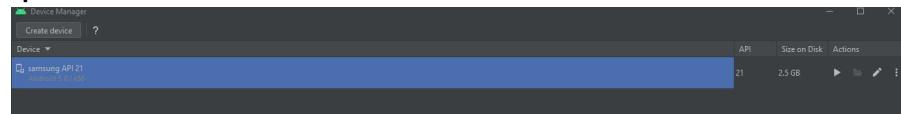
➤ Step 14:- select any one android version and click next

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





- Step 16:- AVD device created

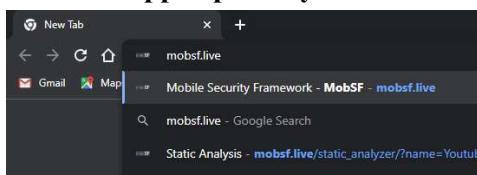


17. Scan any 5 android apps and analyse the report's using MobSF

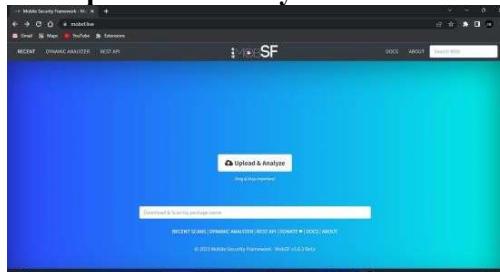
- Step 1:- go to any one browser and download any 5 android apps like “youtube go,Instagram lite,fb lite, snaptube,dr driving”



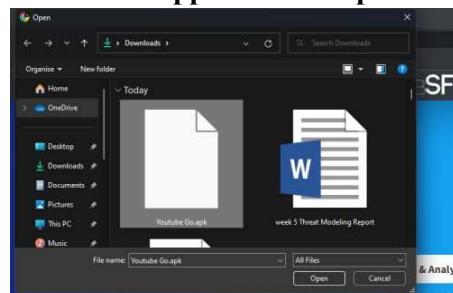
- Step 2:- after download the apps open any browser and search “mobSF.live”



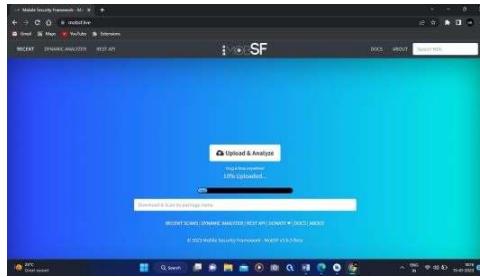
- Step 3:- Then click on upload and analyse



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



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

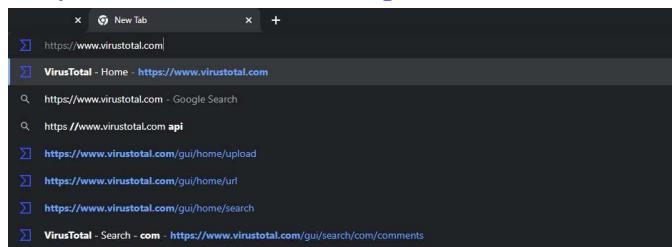


- Step 6:- after complete the analyse click on pdf report and save the report and analyse thereport

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

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

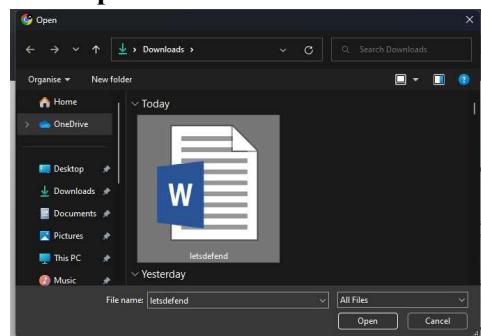
- Step 1:- Go to any browser and search <https://www.virustotal.com>



- 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



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.

19. 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

The screenshot shows a Google search results page for the query "letsdefend". The top result is a link to "LetsDefend - Blue Team Training Platform" with a brief description: "LetsDefend helps you build a blue team career with hands-on experience by investigating real cyber attacks inside a simulated SOC". Below the link are two other links: "Login" and "Training".

- Step 2: Click on Sign-Up

The screenshot shows a dark-themed web page for "SOC Analyst Training". At the top, there are navigation links for "Testimonials", "Blog", "Contact", "Login", and a prominent "Sign-Up" button. The main content area features the text "SOC Analyst Training" and a large blue circular graphic.

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

The screenshot shows a sign-up form titled "free account". It includes fields for "Email" (yashaswini), "Password", "Choose Country" (India selected), and a checkbox for "I agree to the terms and conditions". A "Get Started" button is at the bottom. The background features a large blue circular graphic.

- Step 4: Click on Start

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

• Took 30 sec // windows
Use to activate Windows.
Start

- Step 5: choose an answers for the given questions

1> How did you discover LetsDefend? *

A Search engine (Google, Yahoo, etc.)
B Recommended by friend or colleague
C Social media
D Blog or publication
deploma syllabus



OK ✓

2> What is your current role/level? *

A Student
B SOC Analyst
C Manager / Team Leader
D C Level / Founder
E Security Engineer
F Other

OK ✓

3> How much time do you spend improving your technical knowledge? *

A Every day
B A few times a week
C A few times a month
D Other

OK ✓

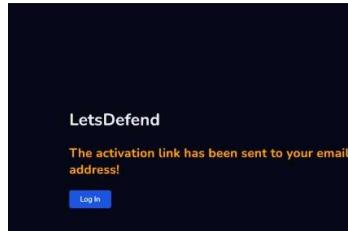
4> What would you expect from a training platform? *

You can choose 1 more

A Quality contents
B Hands-on exercises
C Real world compatibility
D Ease of Use
E Lots of training material

Submit

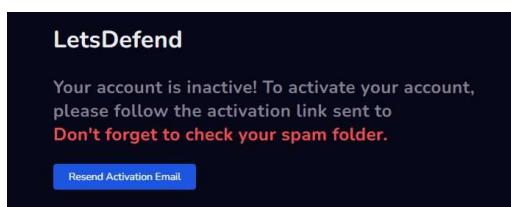
➤ Step 6: Click on log in



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



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

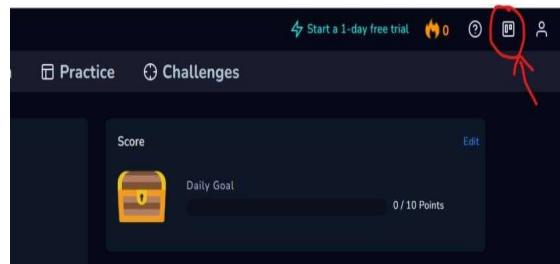


Hi yashu,

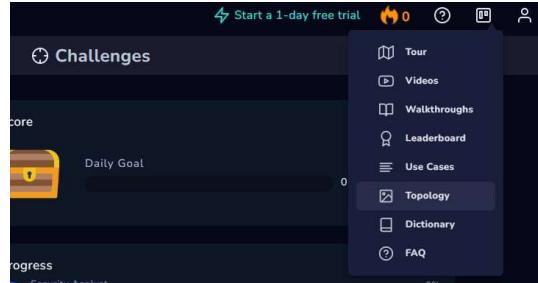
Please click on the link to confirm your registration to LetsDefend.
If you think, it's not you, then just ignore this email.

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

