PROTECTING YOUR COMPUTING DEVICES:

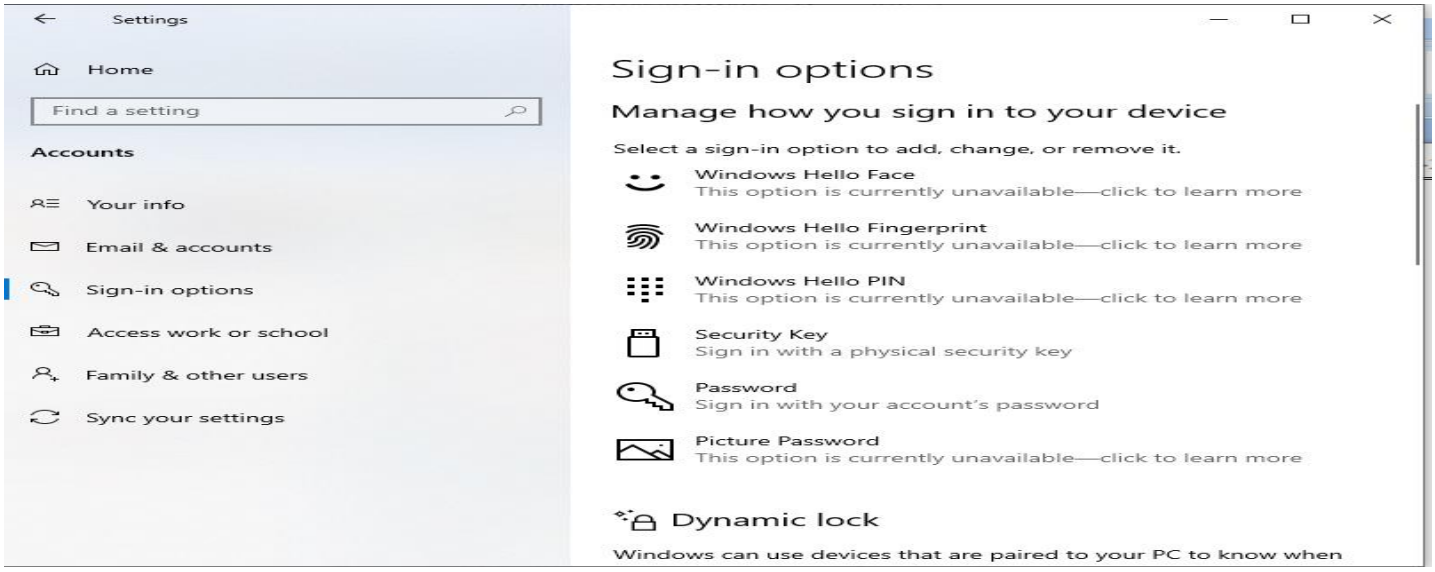
a) Set up password

b) Turn On windows Firewall

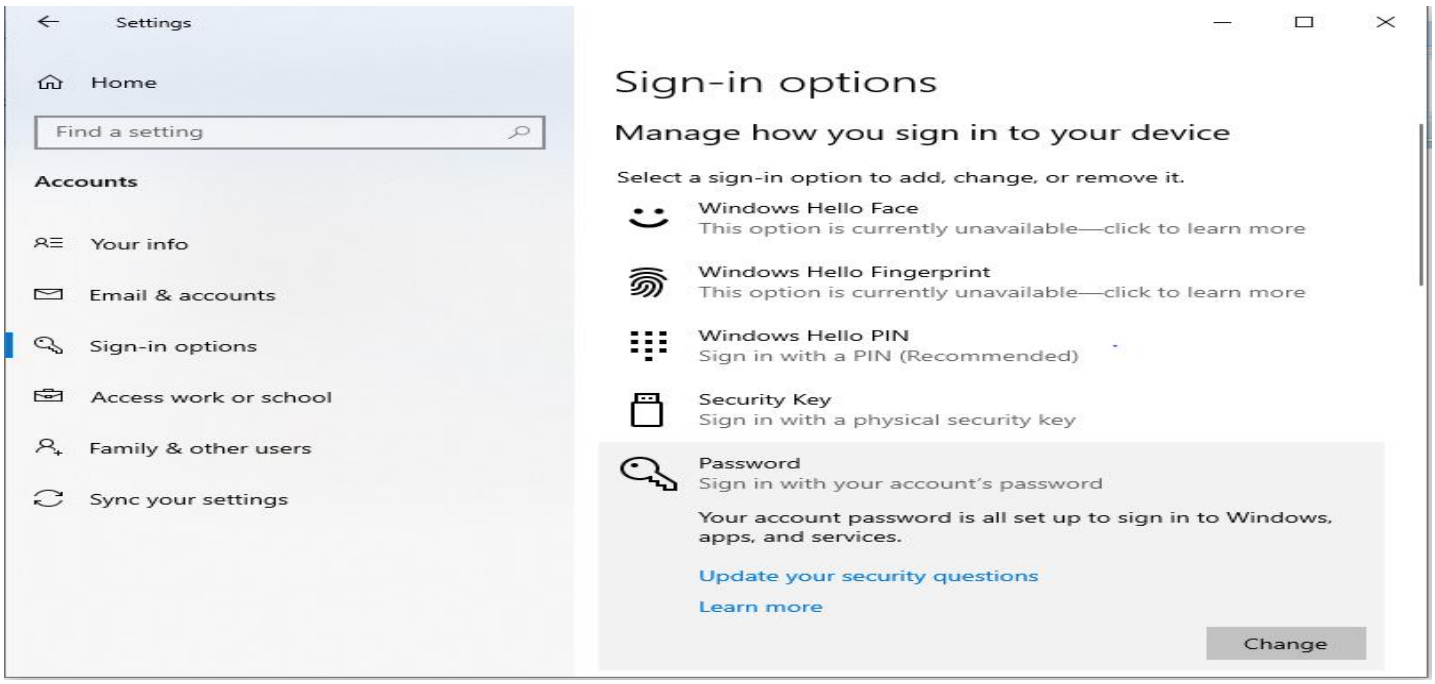
c) Install and Scan Antivirus

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

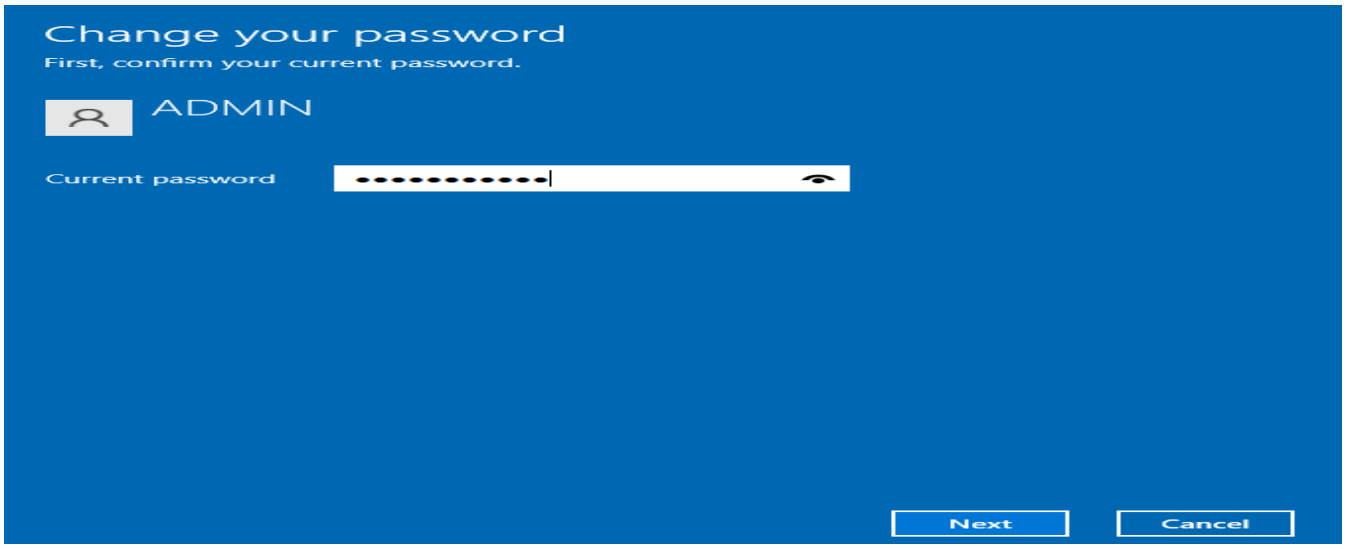
- Step1:- press the windows 1o keyboard shortcut “windows + I” to open the setting app. Now, move toaccounts-> sing-in option.



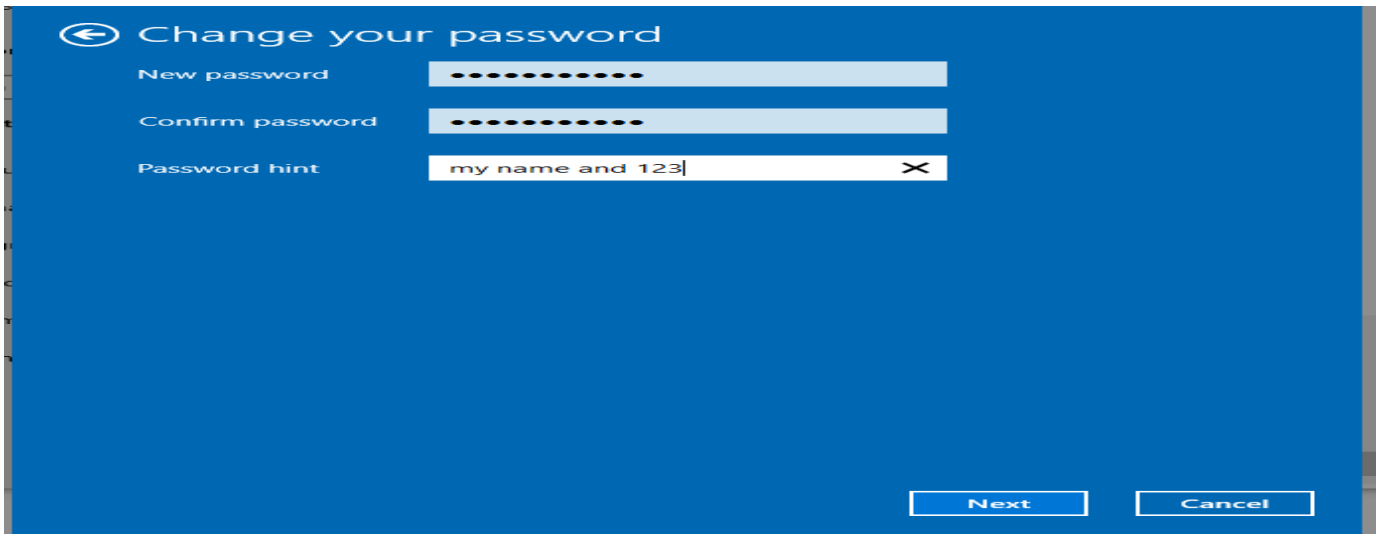
- Step2:-here click to expand the “password” section and then click the “change pin” button.



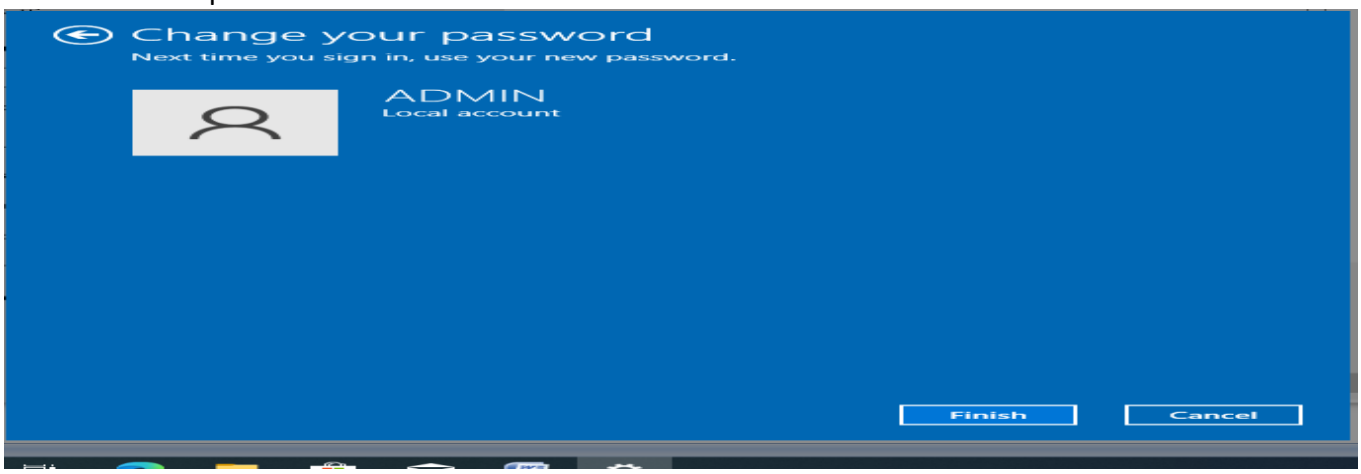
- Step3:-after that enter the current password of your windows 10 pc and click on “next”.



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



- Step5:- finally click on “finish”, and you are done. You have successfully changed your windows 10password.

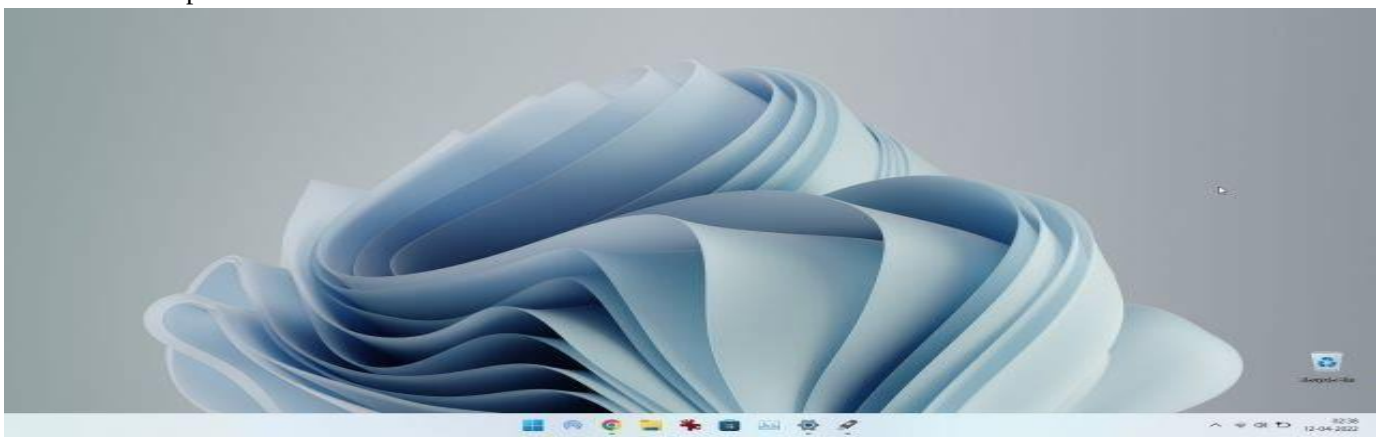


Check windows update and update the system:

- 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.

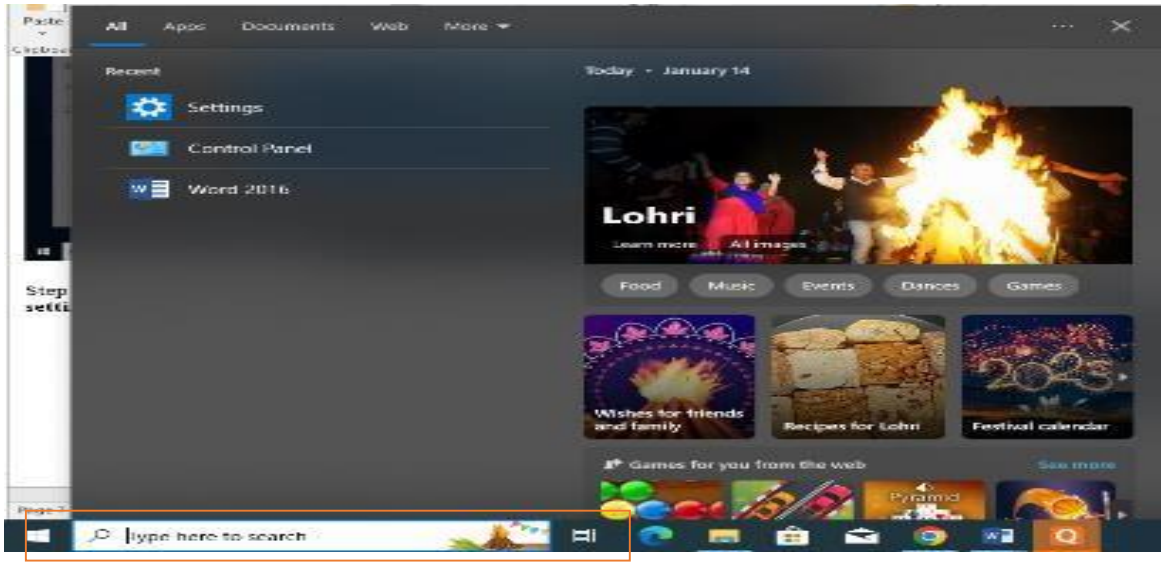
- Step2 :- once here, click on “check for updates”. If there is an update available, it will show up here and will be downloaded automatically.

- 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.

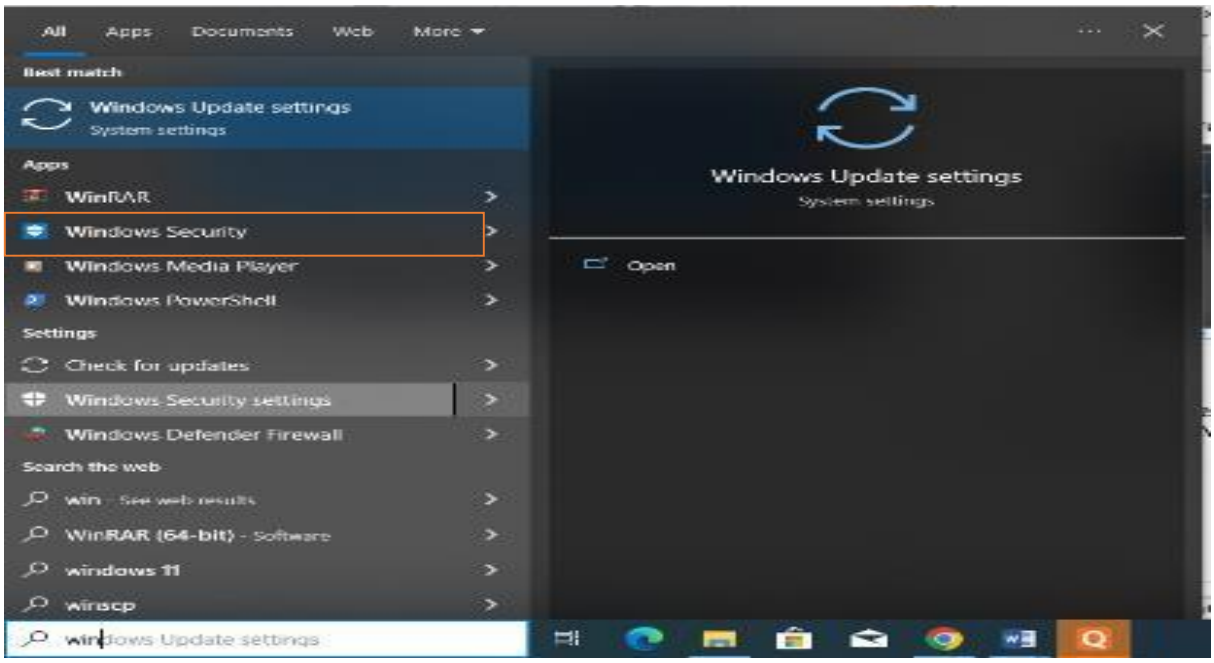


b) Demonstrate Turn on & off Windows OS Firewall

- Step 1: go to search

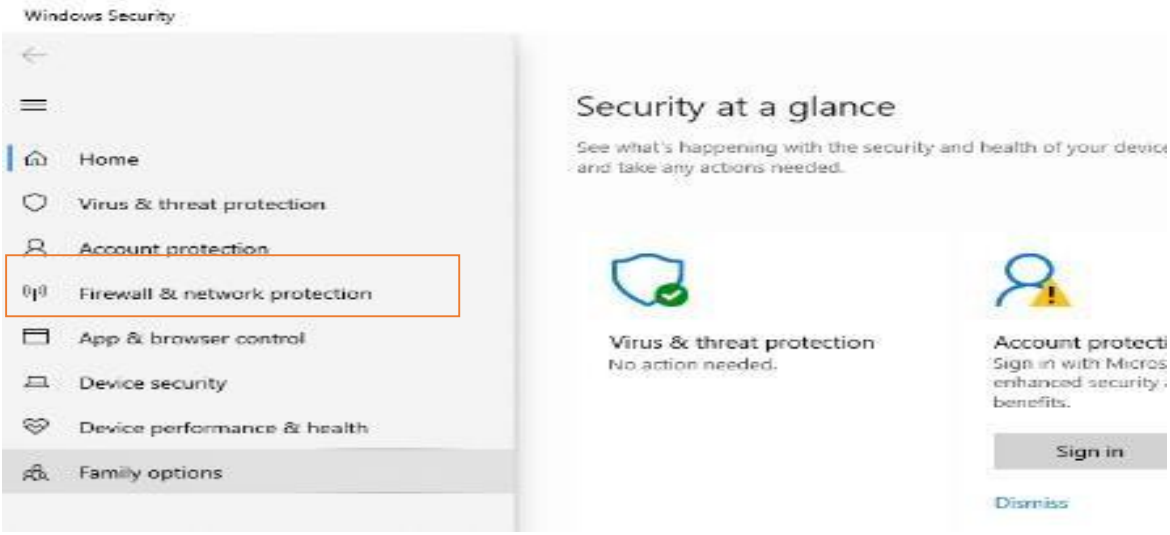


- Step 2: search windows security



- Step 3: Click on Navigation button

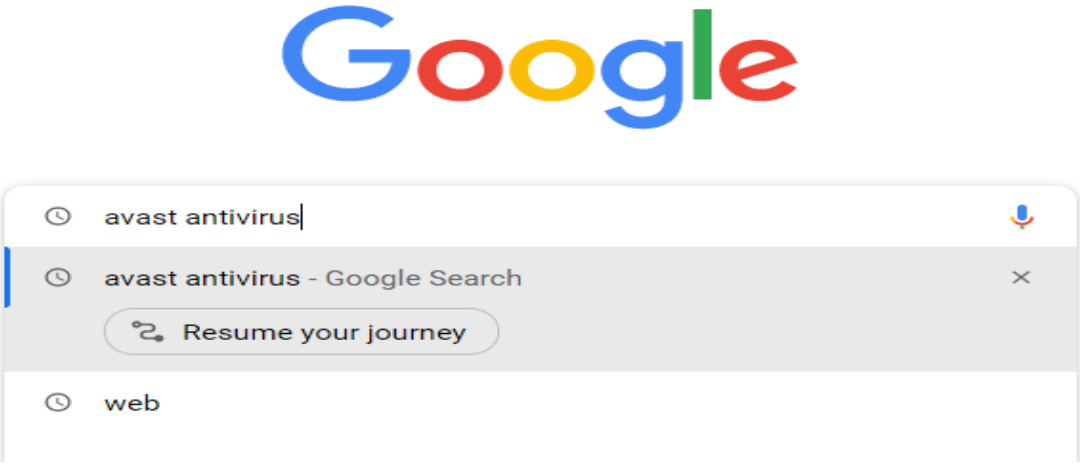
- Step 4: Click on Firewall and network protection



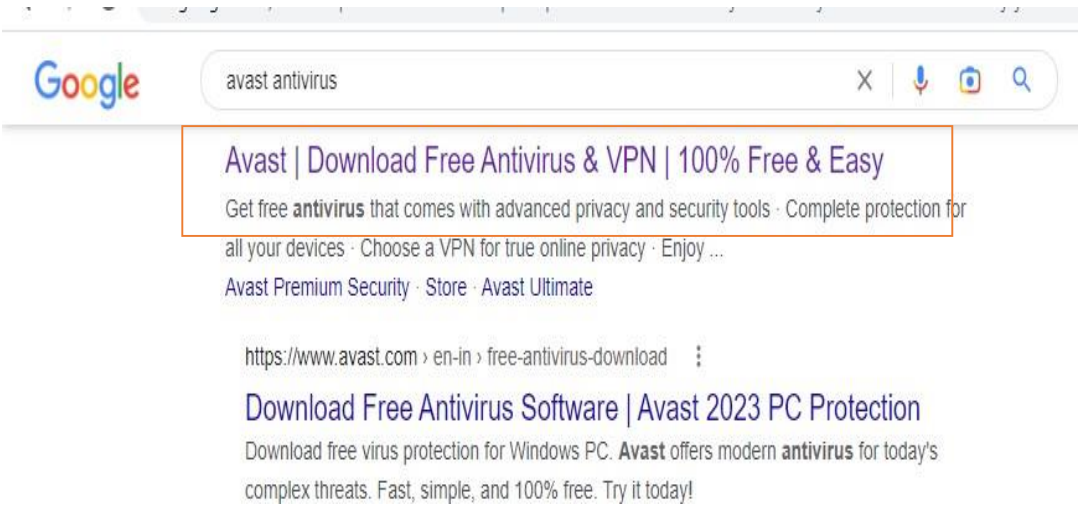
- Step 5:- if you installed any anti-virus software's the firewall will open in app , now you can on & the firewall

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

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

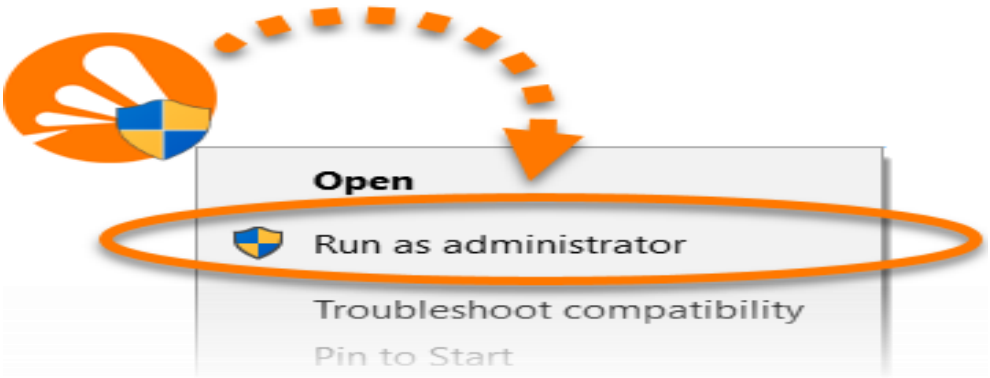


- Step 2:- click on avast download free antivirus & vpn link

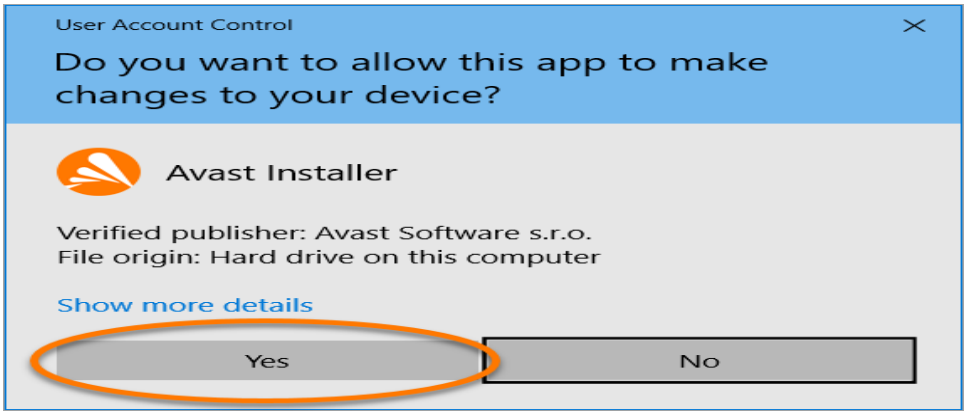


- Step 3:- click on Download free protection button

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

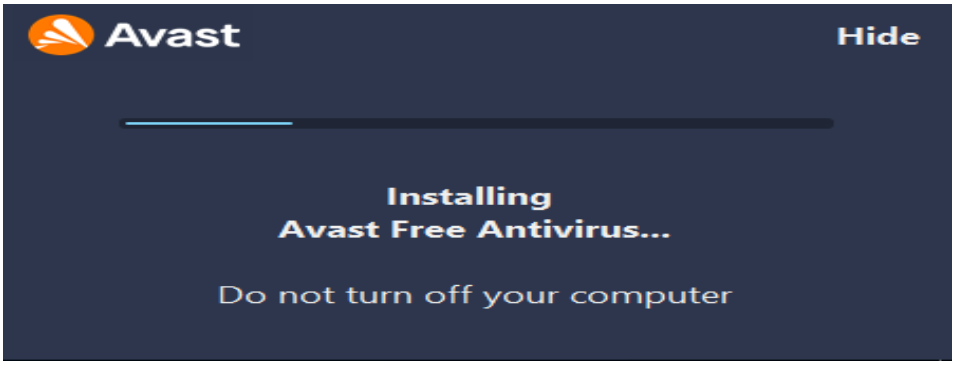


- Step 5: If prompted for permission by the User Account Control dialog, click Yes.

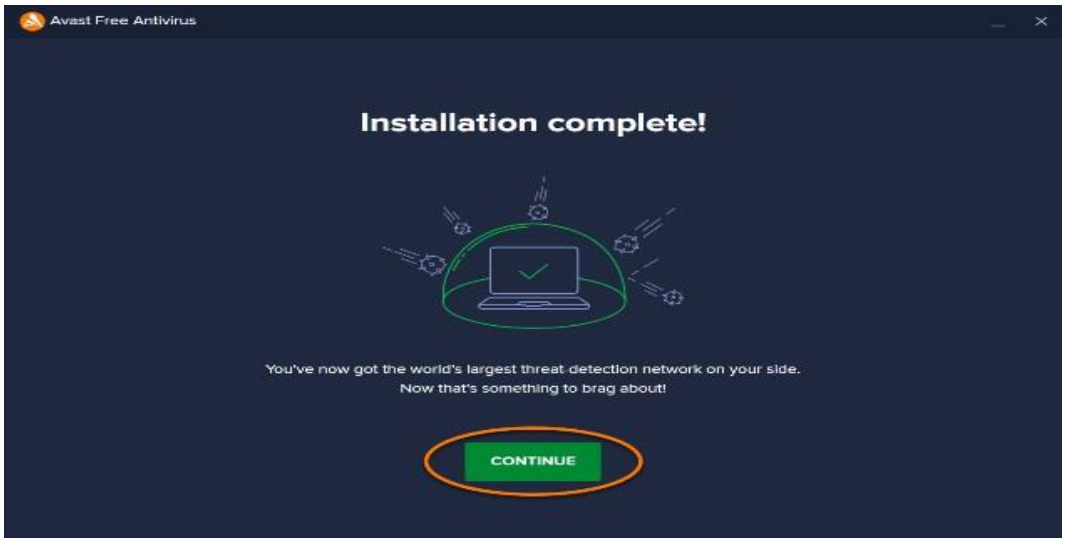


- Step 6: Then, click Install

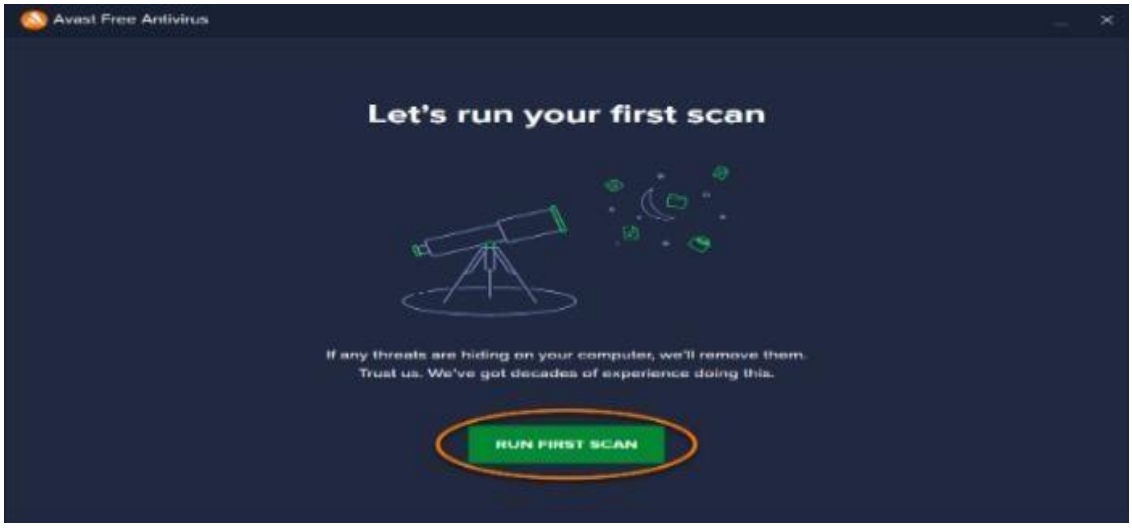
- Step 7: Wait while setup installs Avast Free Antivirus on your PC.



- 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 copiesof 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

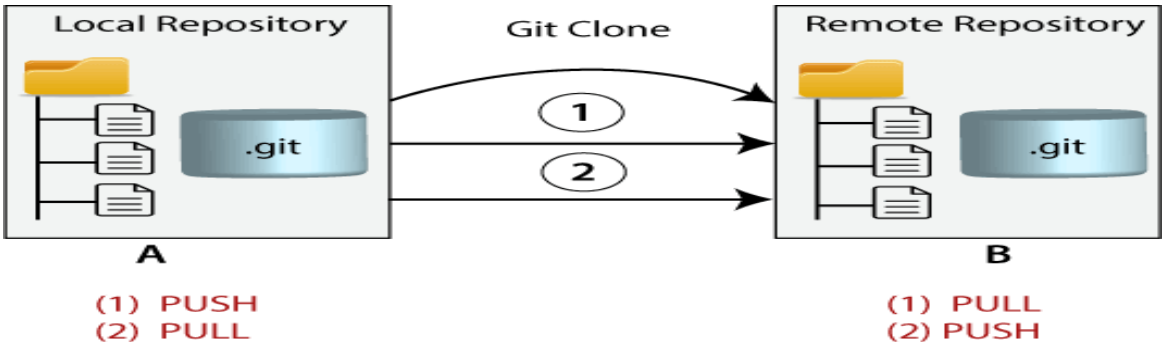
commit 7fb5597a03108100aa665d985d5183d9704e1367
Author: lohith <lohith123@gmail.com>
Date: Thu Jul 20 11:44:37 2023 +0530

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:

1: Before pushing local file to remote location or GitHub , we have to first add and commit file.Step

2. 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_sFhFsSHhTzMDreGRLjmks4Tzuzgthdvfsrta`

3: 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.

S 3: 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/lohithgithub/soraba.git
remote:
remote: Create a pull request for 'master' on GitHub by visiting:
remote:      https://github.com/lohithgithub/soraba/pull/new/master
remote:
To https://github.com/lohithsy/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 tothis 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:

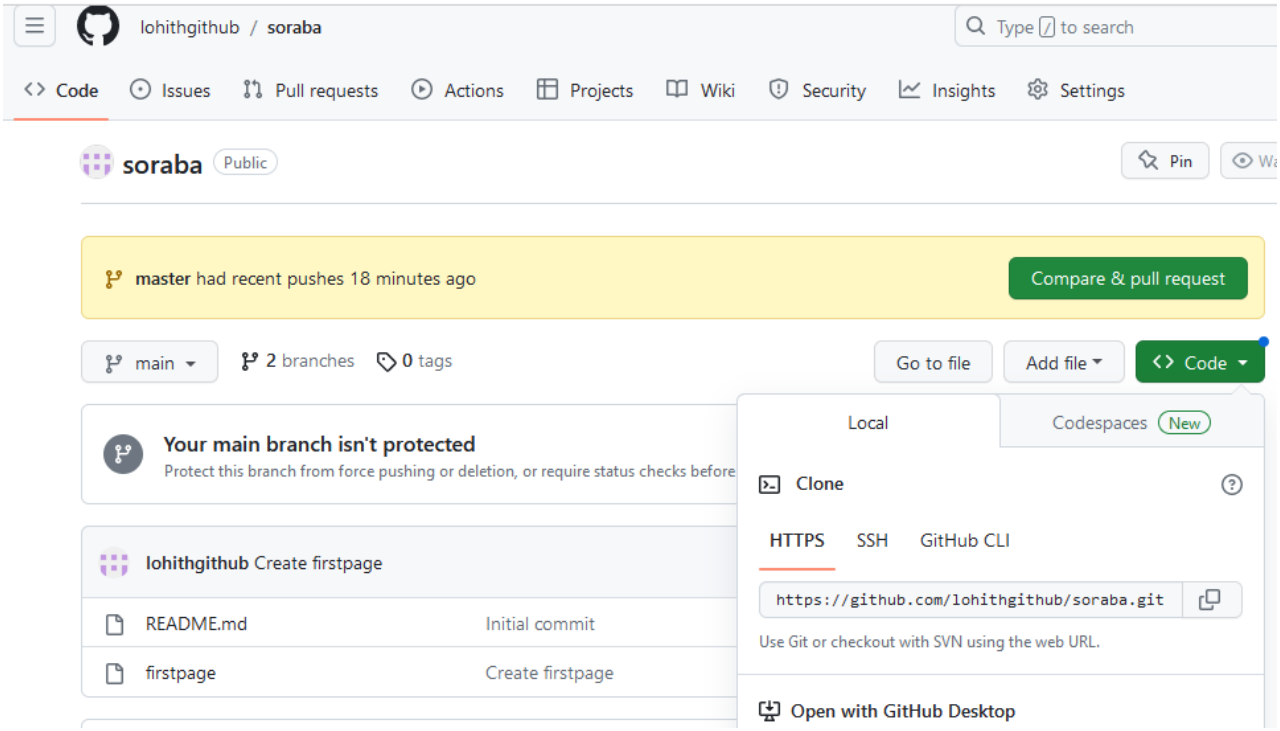
Step 1: Open GitHub website and login with user account and navigate to the main page of the repository.

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
```

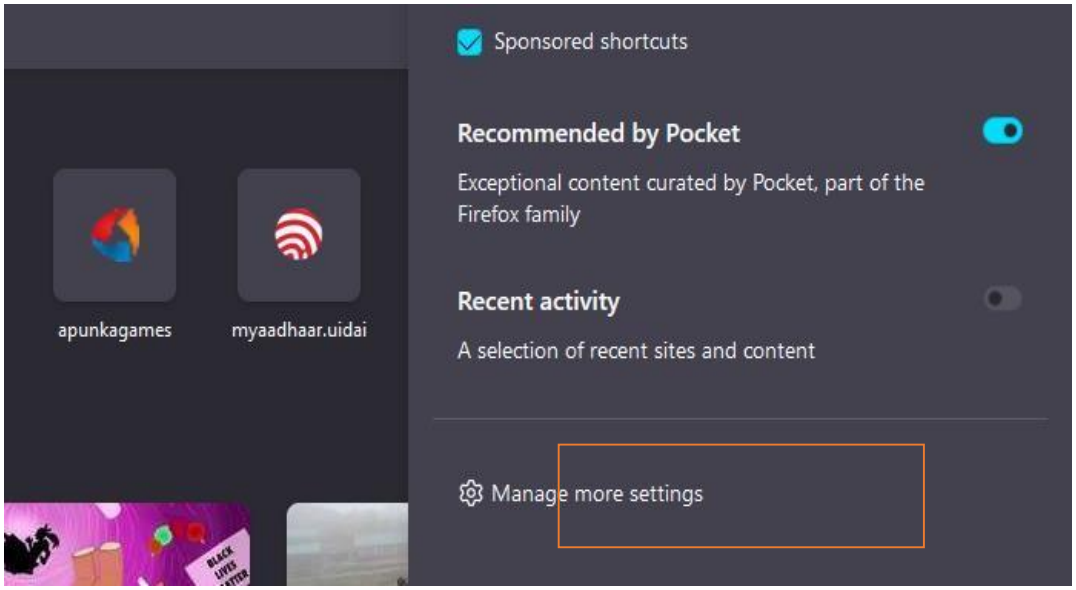
Step 7: Now go to the test folder where you have downloaded repository called soraba from remote location.

Check the browser and website certificates and analyse the certificates

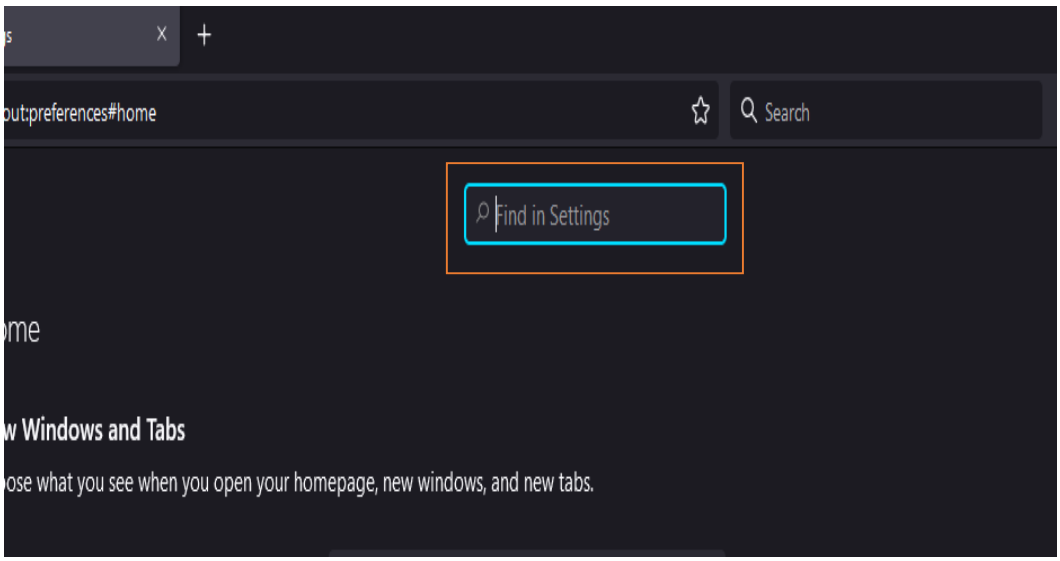
Browser certificates view:

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

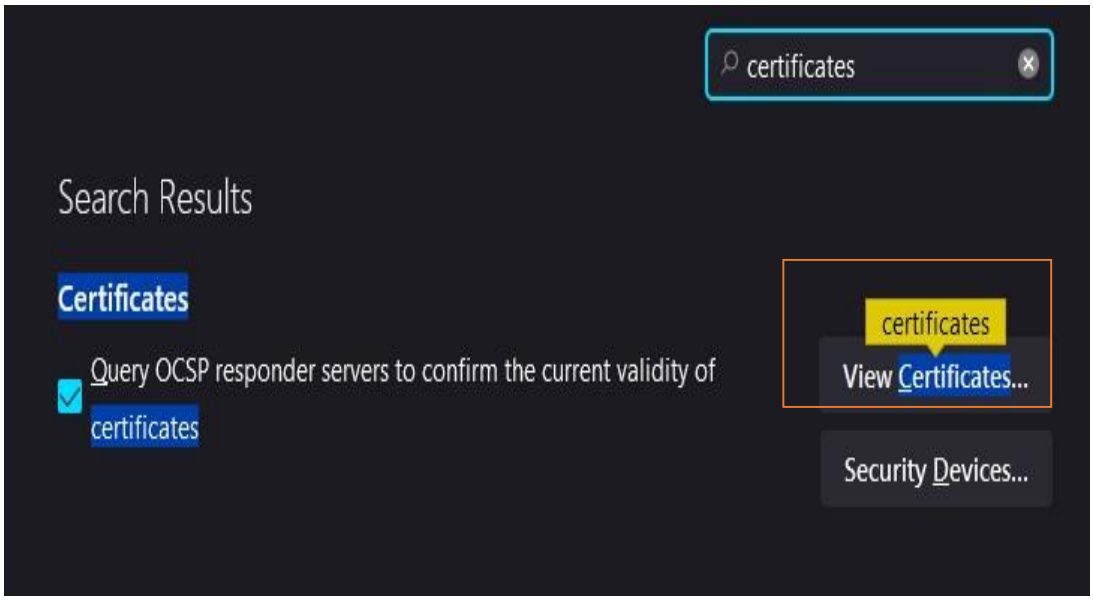
- Step 2:- click manage more setting option



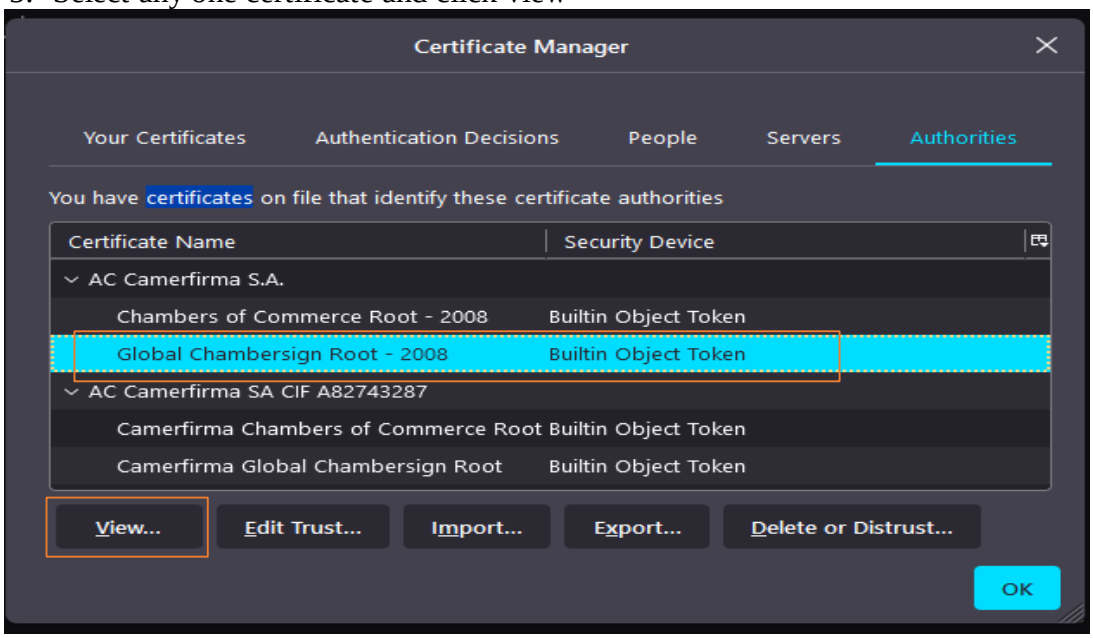
- Step 3:- Search certificates in search box



- Step 4:- Click on view certificates



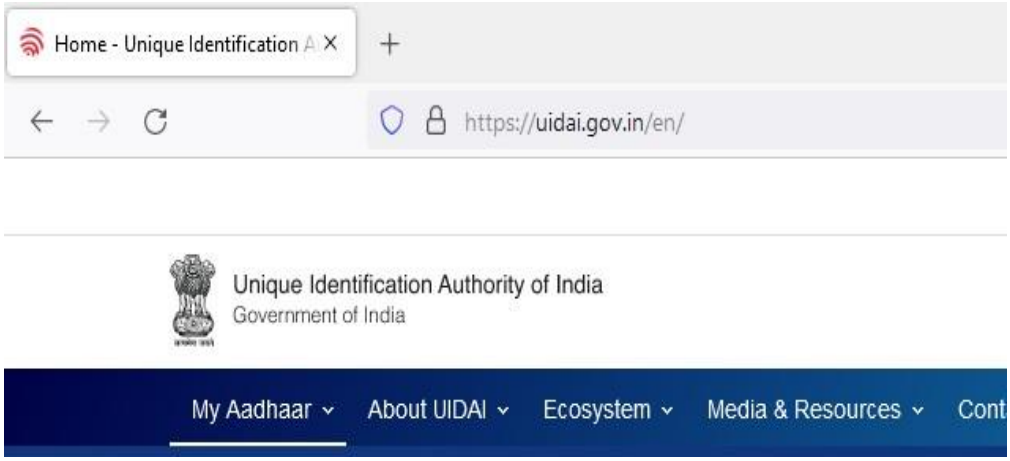
- Step 5:- Select any one certificate and click view



- Step 6:- Now you can see the certificate

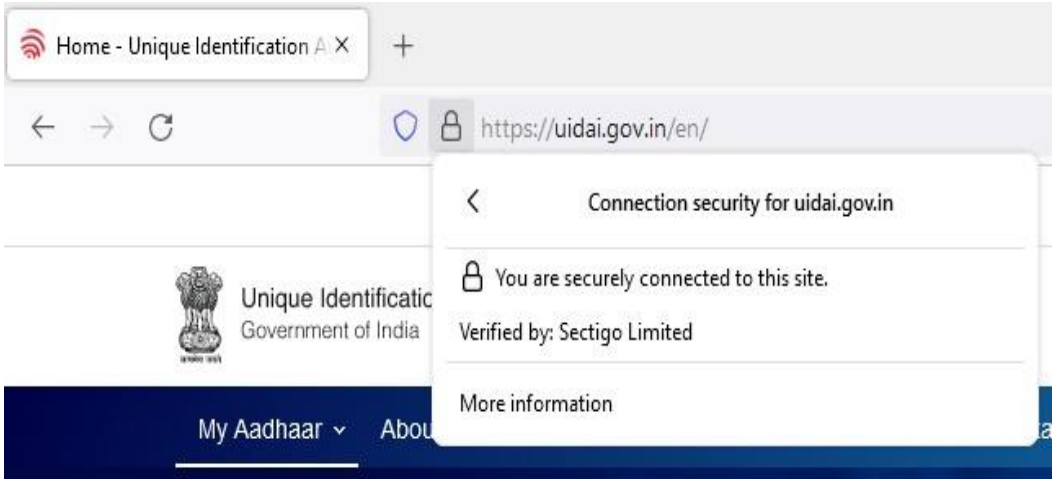
Website certificate check:

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

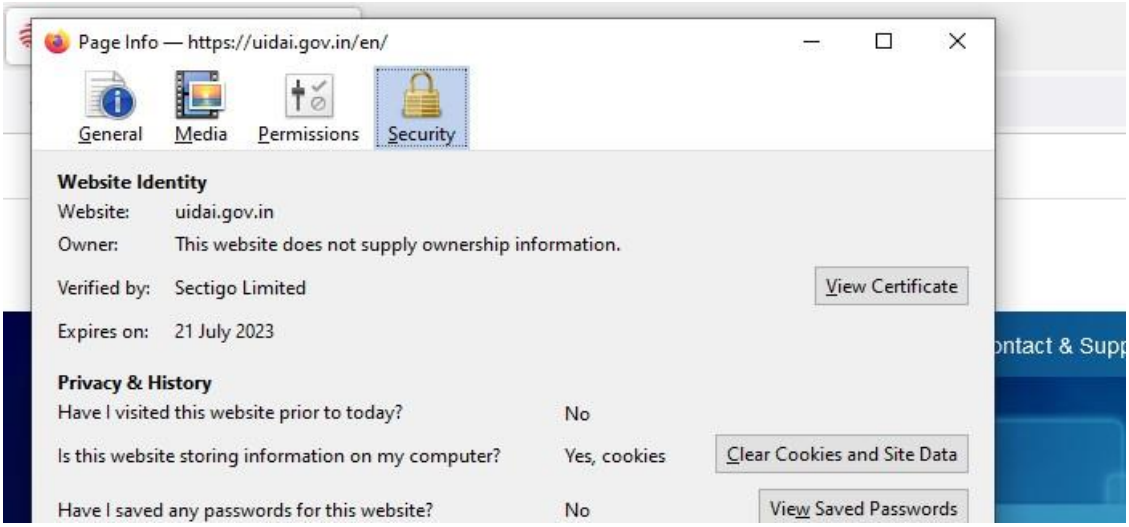


- Step 3:-Click connection secure

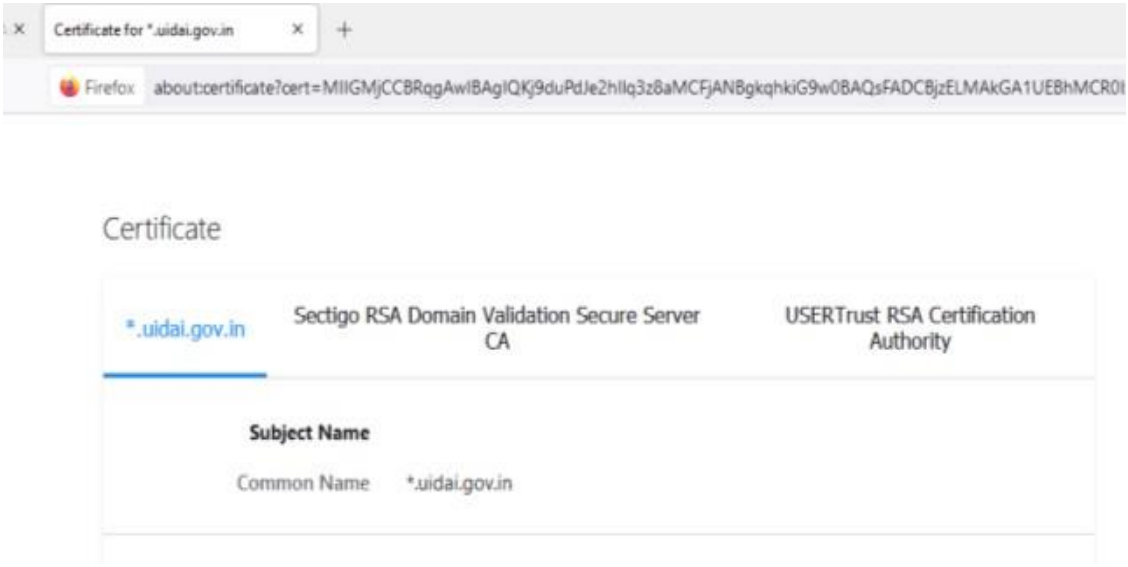
- Step 4:- Click more information



- Step 5 :- Now click view certificate



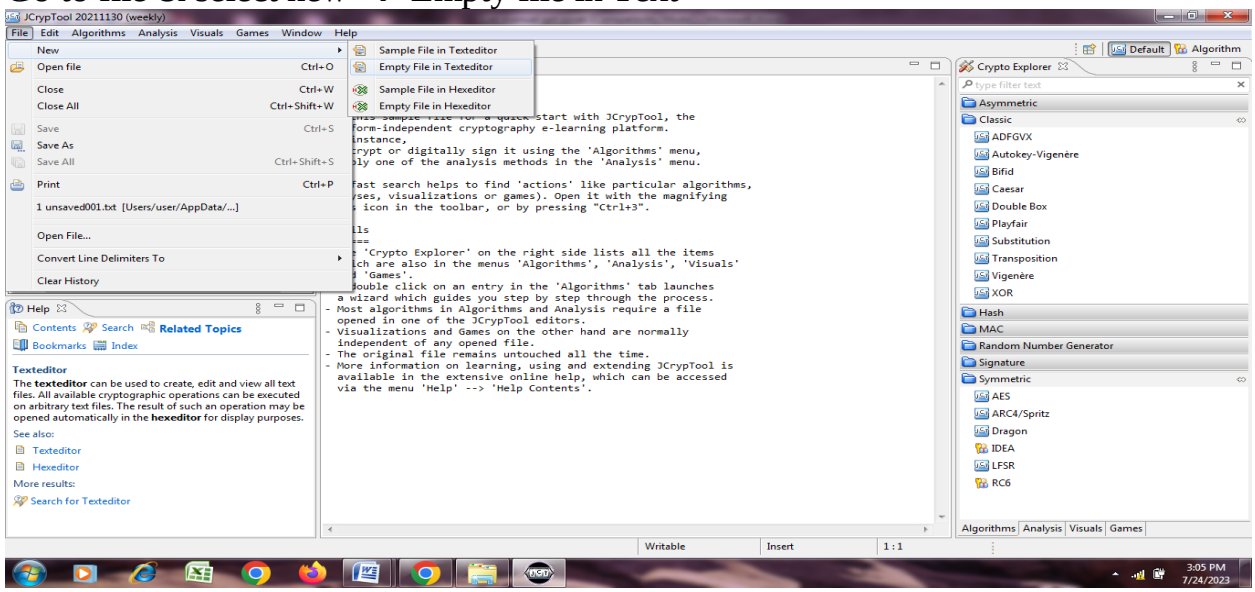
- Step 6:- Now you can see the certificate details



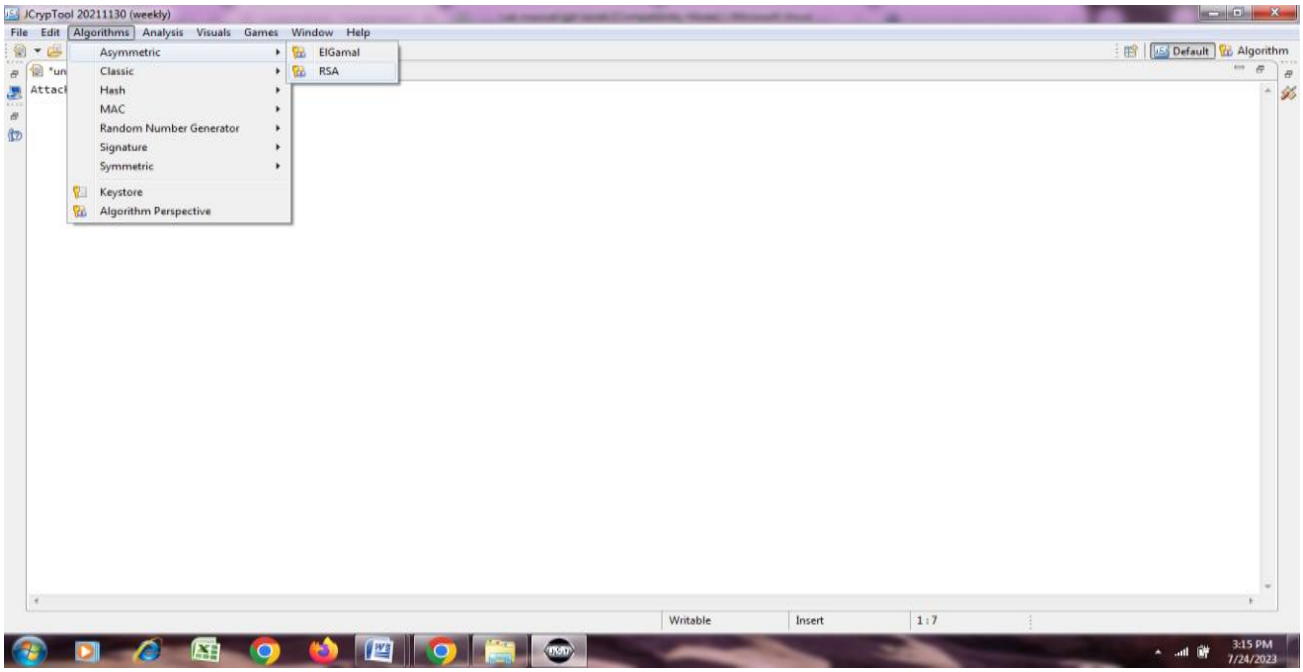
Install JCrypt Tool and demonstrate Asymmetric, Symmetric crypto algorithm, Hash and Digital signatures.

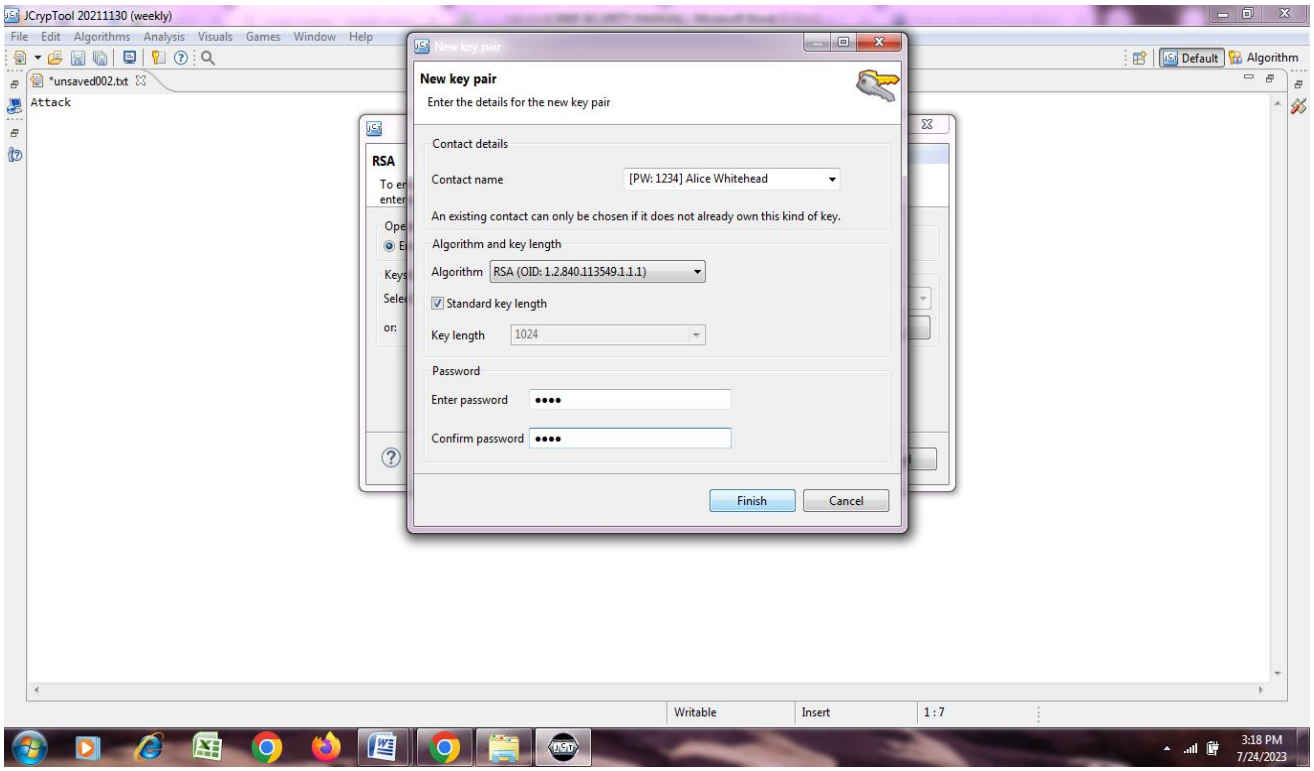
Steps for Encryption:

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

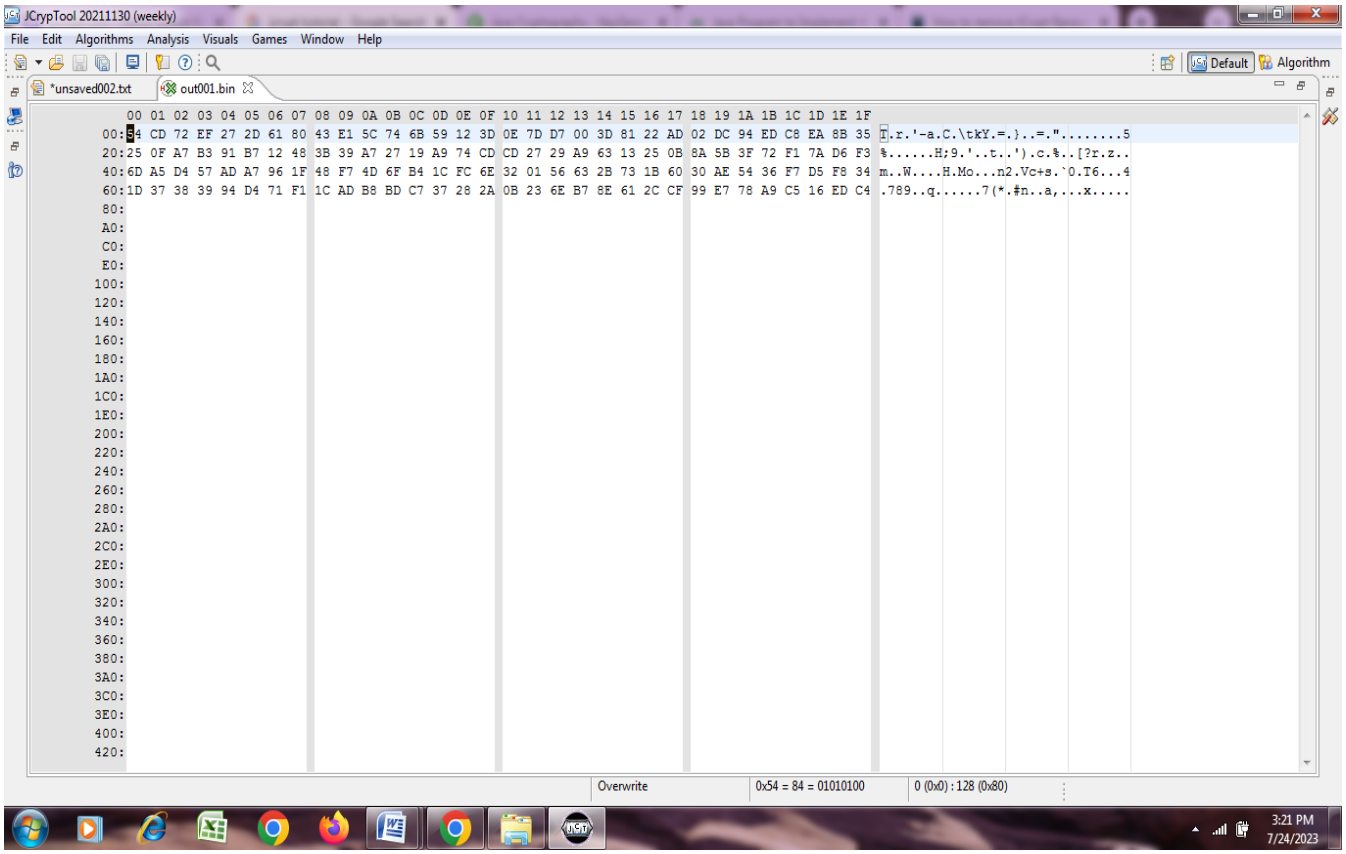


- Then type the message
- Go to Algorithms select Asymmetric →RSA
- *Select Encryption Generate New Pair of Key →Enter Password*

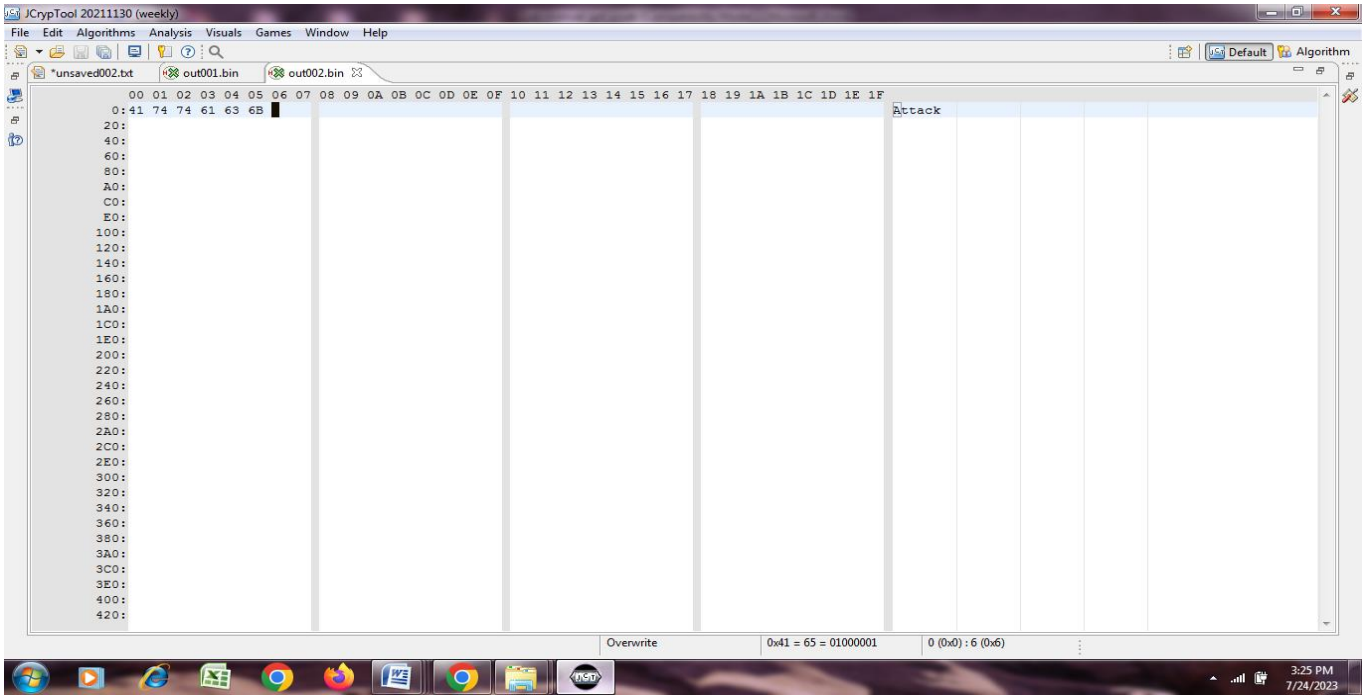




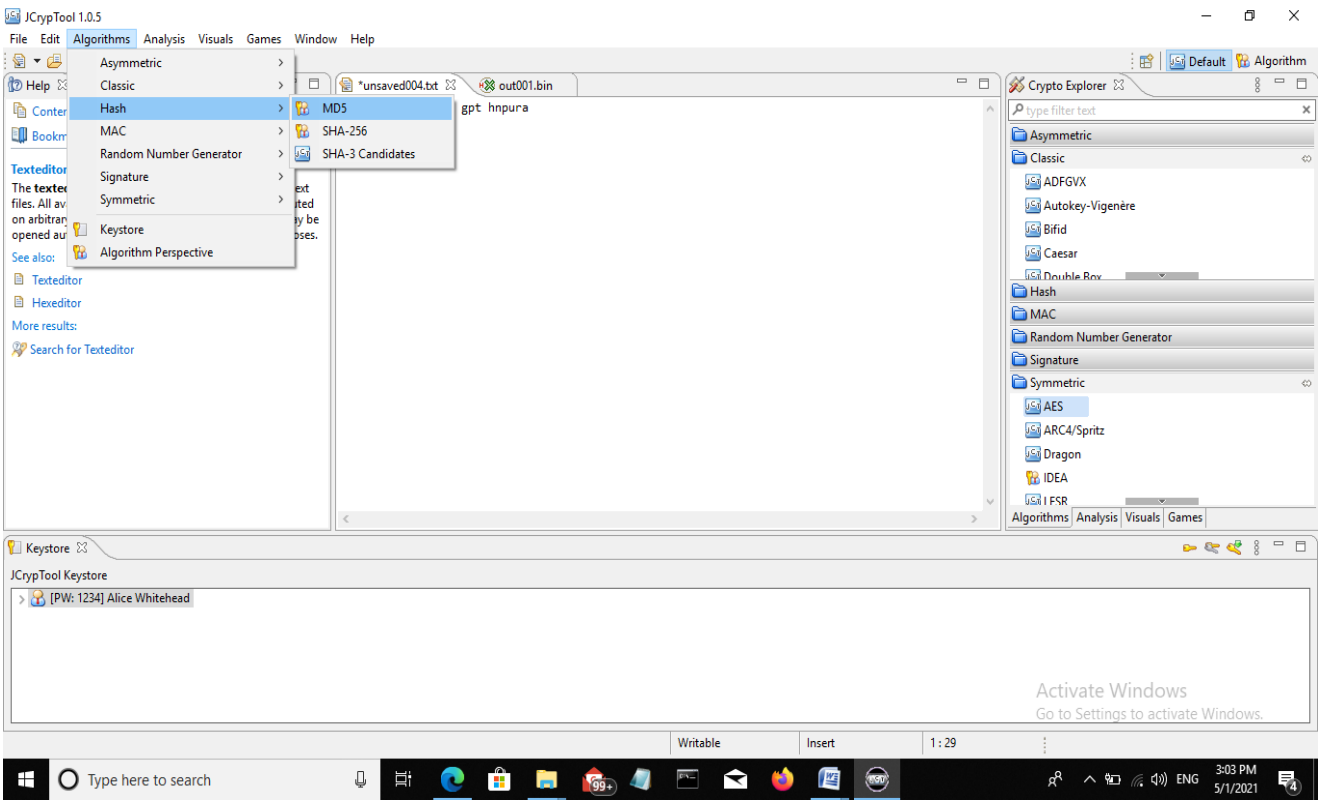
- Then your message will be encrypted

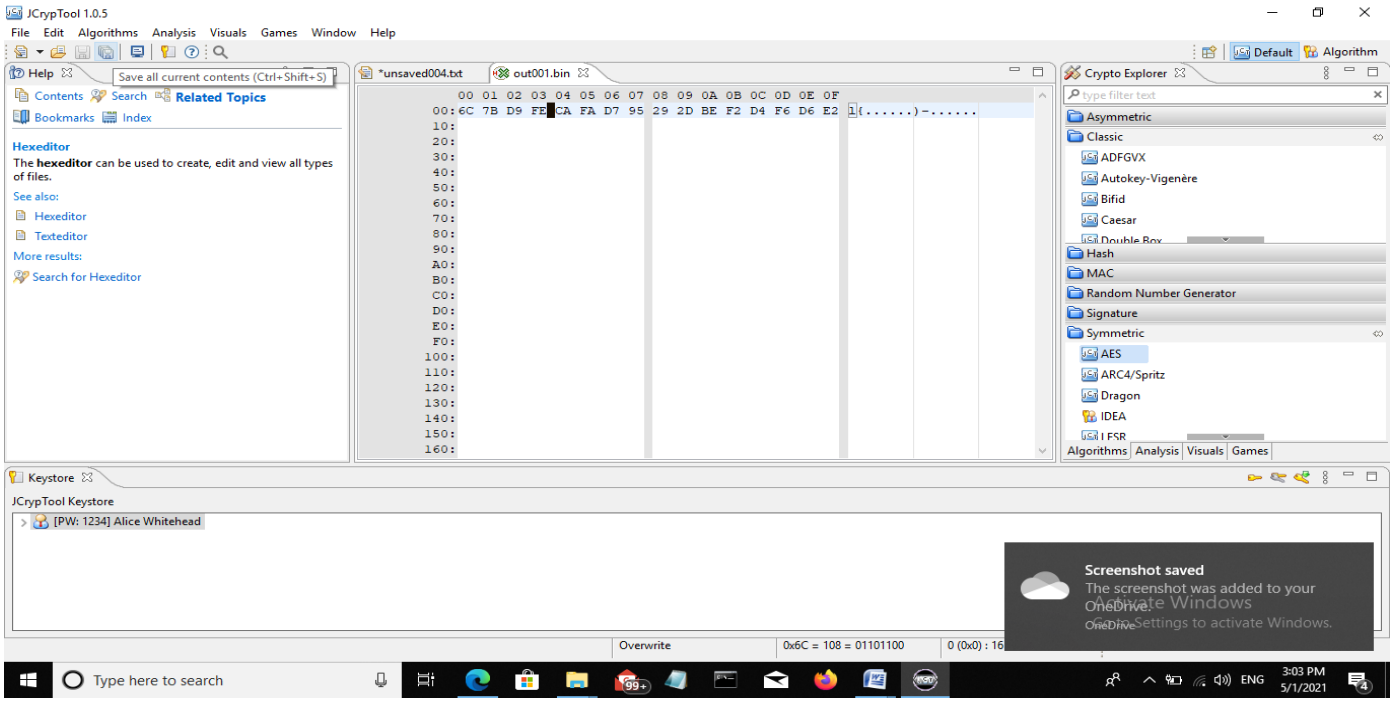


Now Select RSA algorithm and Decryption the message

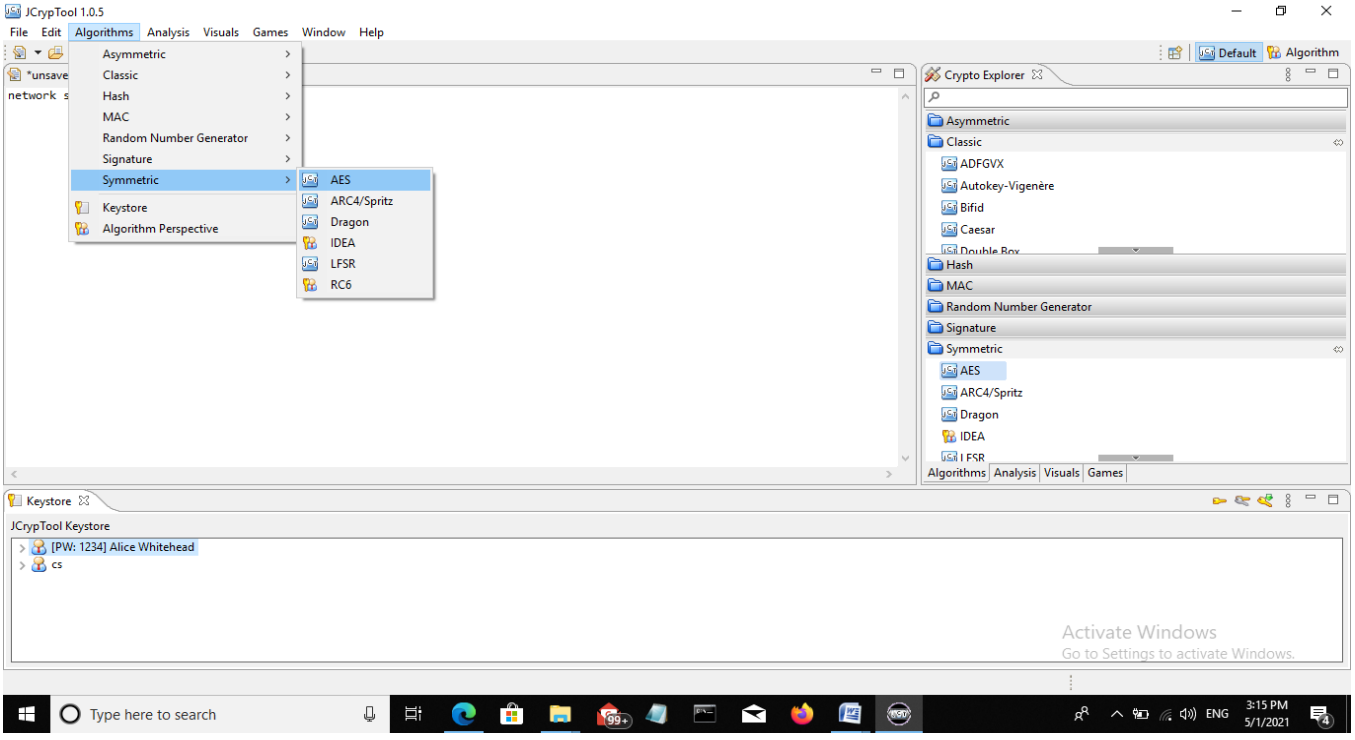


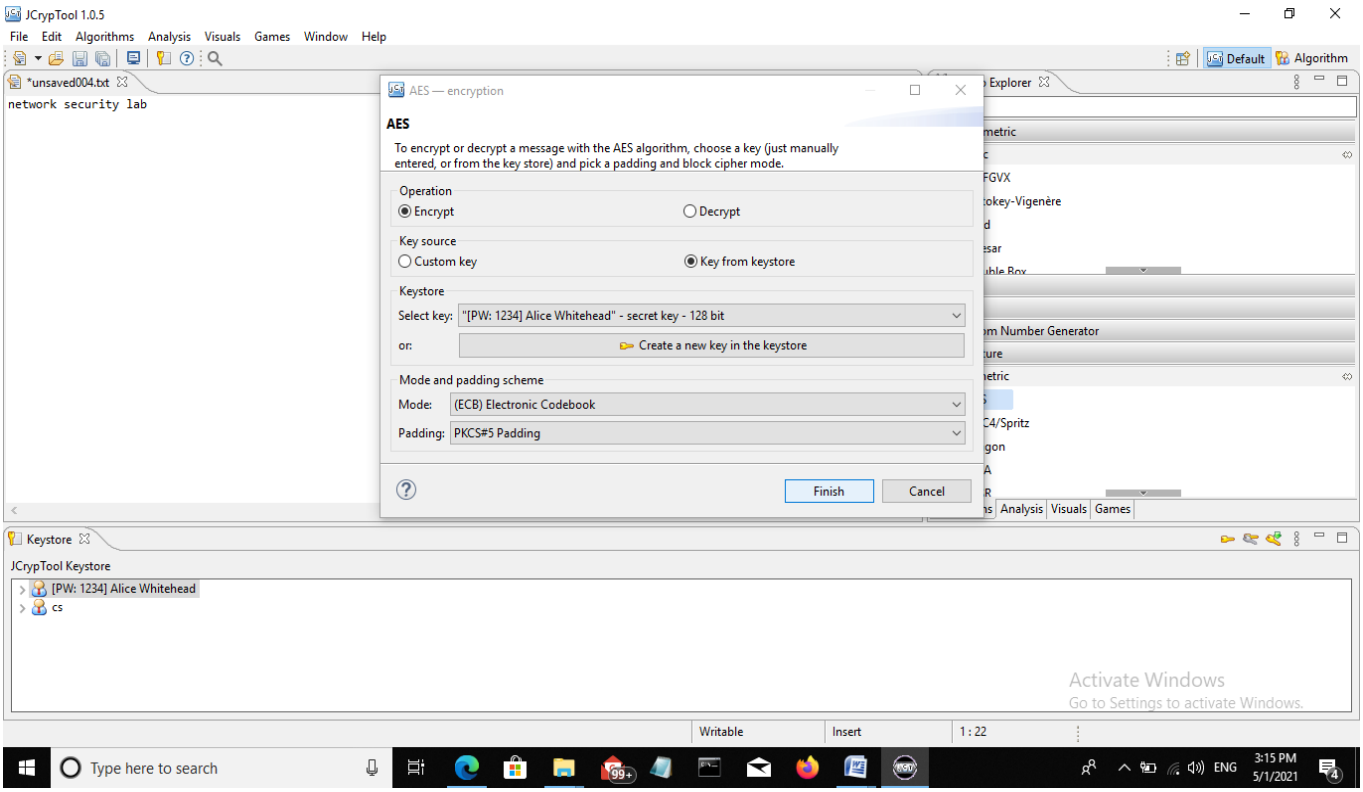
From menu select Algorithm----->HASH------->MD5 and follow steps as in images.

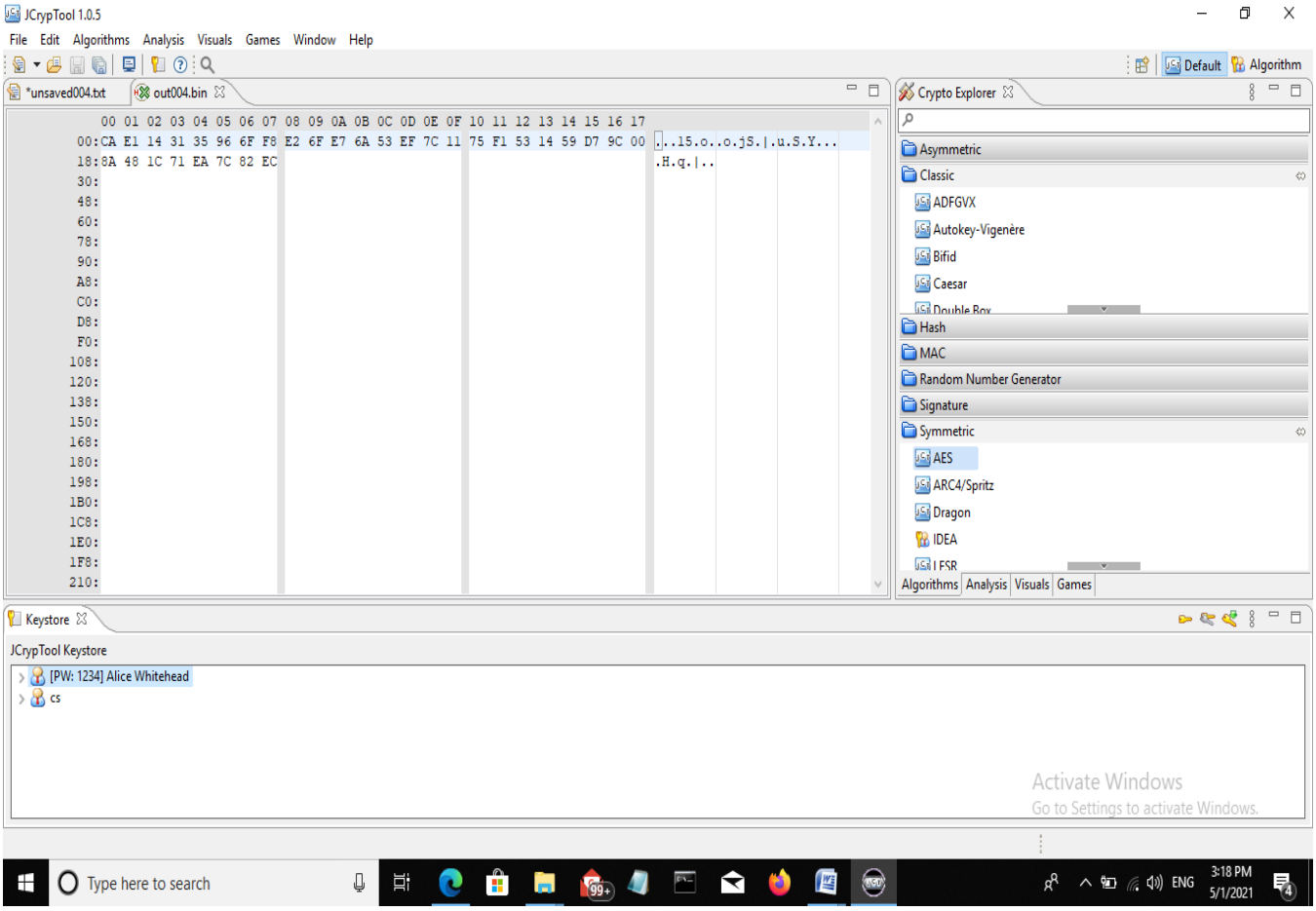


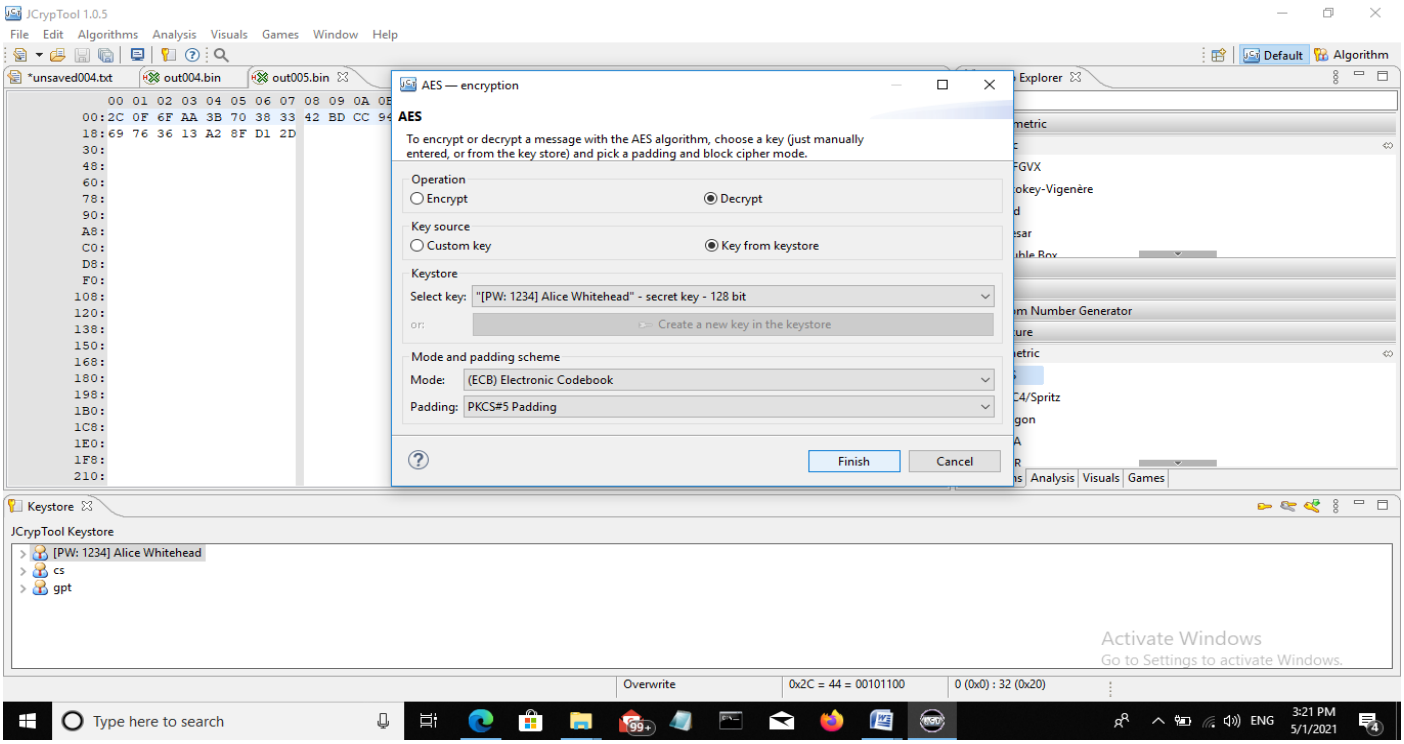


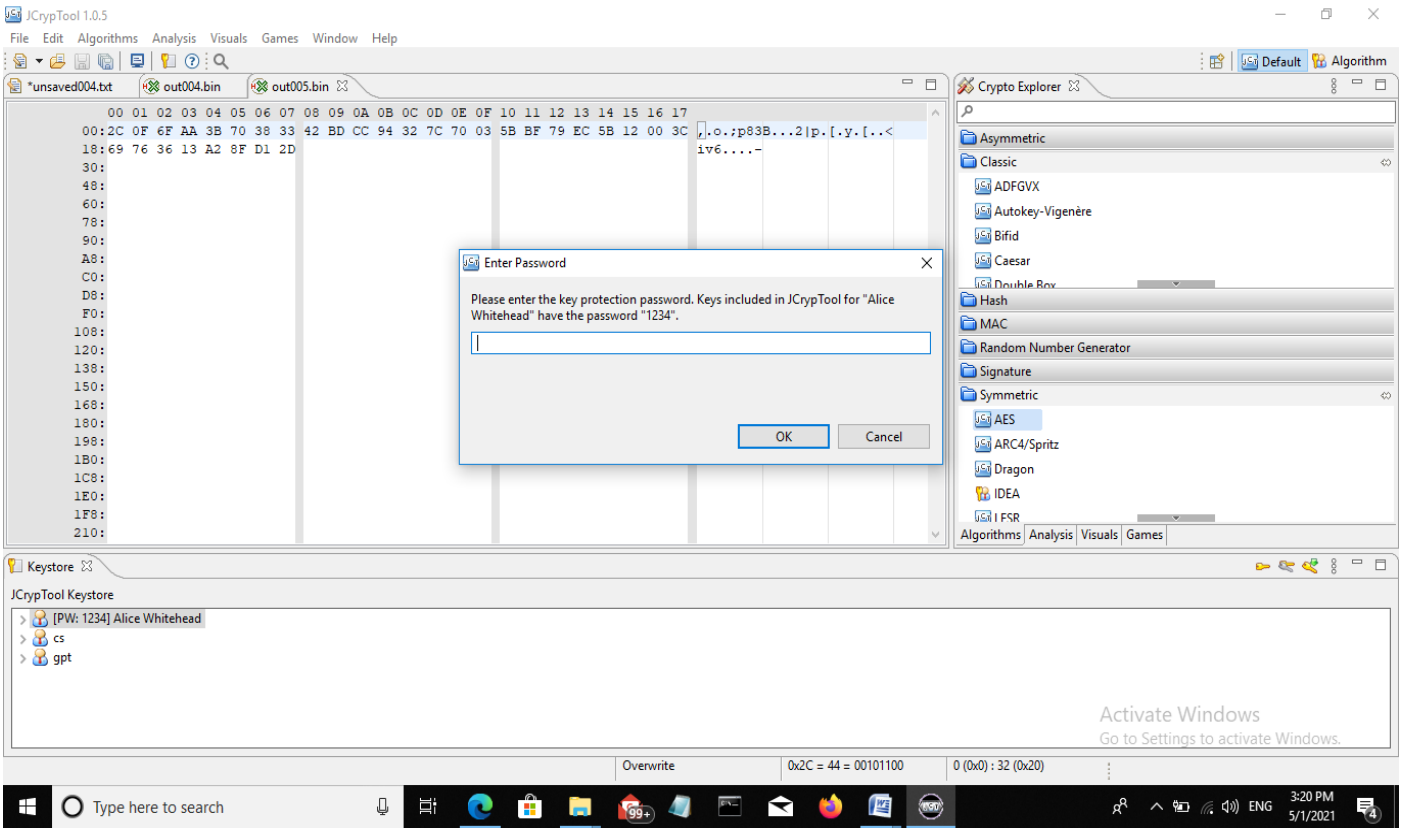
From menu bar select Algorithm------->Symmetric-------->AES and follow steps as in images.

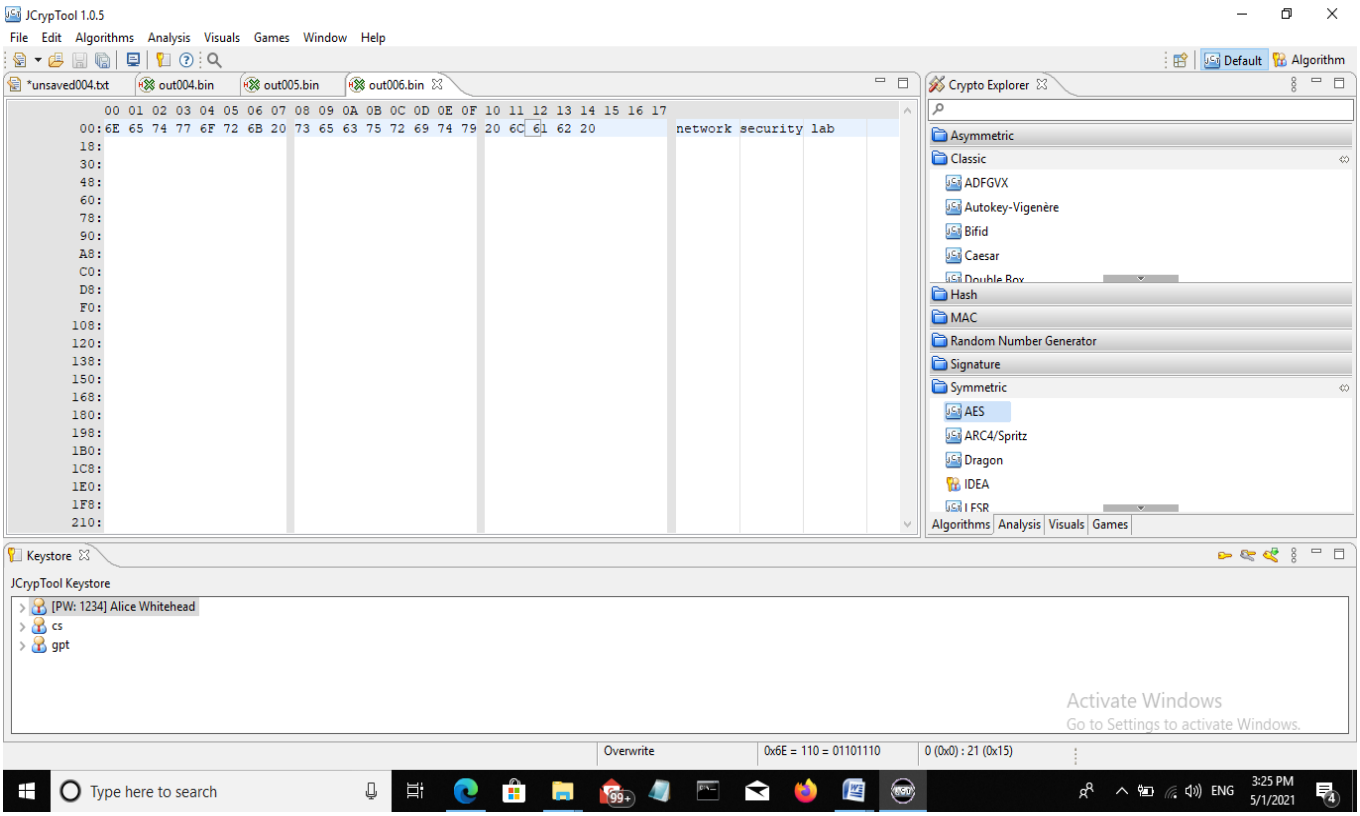



JCrypTool 1.0.5
File Edit Algorithms Analysis Visuals Games Window Help
*unsaved004.txt
network security lab
AES — encryption
AES
To encrypt or decrypt a message with the AES algorithm, choose a key (just manually entered, or from the key store) and pick a padding and block cipher mode.
Operation
Encrypt
Decrypt
Key source
Custom key
Key from keystore
Keystore
Select key: "[PW: 1234] Alice Whitehead" - secret key - 128 bit
or: Create a new key in the keystore
Mode and padding scheme
Mode: (ECB) Electronic Codebook
Padding: PKCS#5 Padding
Finish
Cancel
Keystore
JCrypTool Keystore
[PW: 1234] Alice Whitehead
cs
Activate Windows
Go to Settings to activate Windows.
Writable
Insert
1 : 22
Type here to search
ENG
3:15 PM
5/1/2021

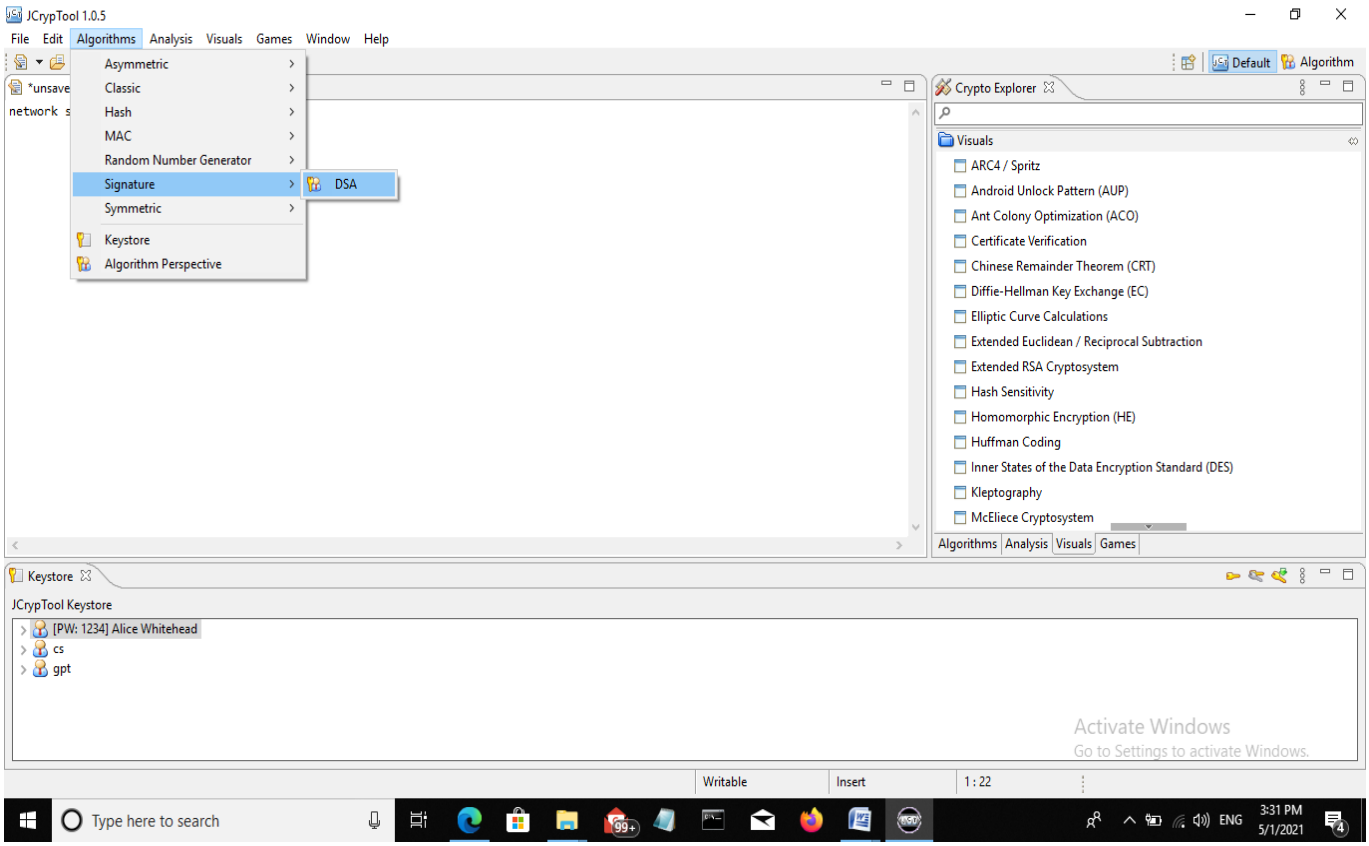

JCrypTool 1.0.5
File Edit Algorithms Analysis Visuals Games Window Help
*unsaved004.txt
out004.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
00:CA E1 14 31 35 96 6F F8 E2 6F E7 6A 53 EF 7C 11 75 F1 53 14 59 D7 9C 00
18:8A 48 1C 71 EA 7C 82 EC
Crypto Explorer
Asymmetric
Classic
ADFGVX
Autokey-Vigenère
Bifid
Caesar
Hash
MAC
Random Number Generator
Signature
Symmetric
AES
ARC4/Spritz
Dragon
IDEA
Algorithms
Analysis
Visuals
Games
Keystore
JCrypTool Keystore
[PW: 1234] Alice Whitehead
cs
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
3:18 PM
5/1/2021

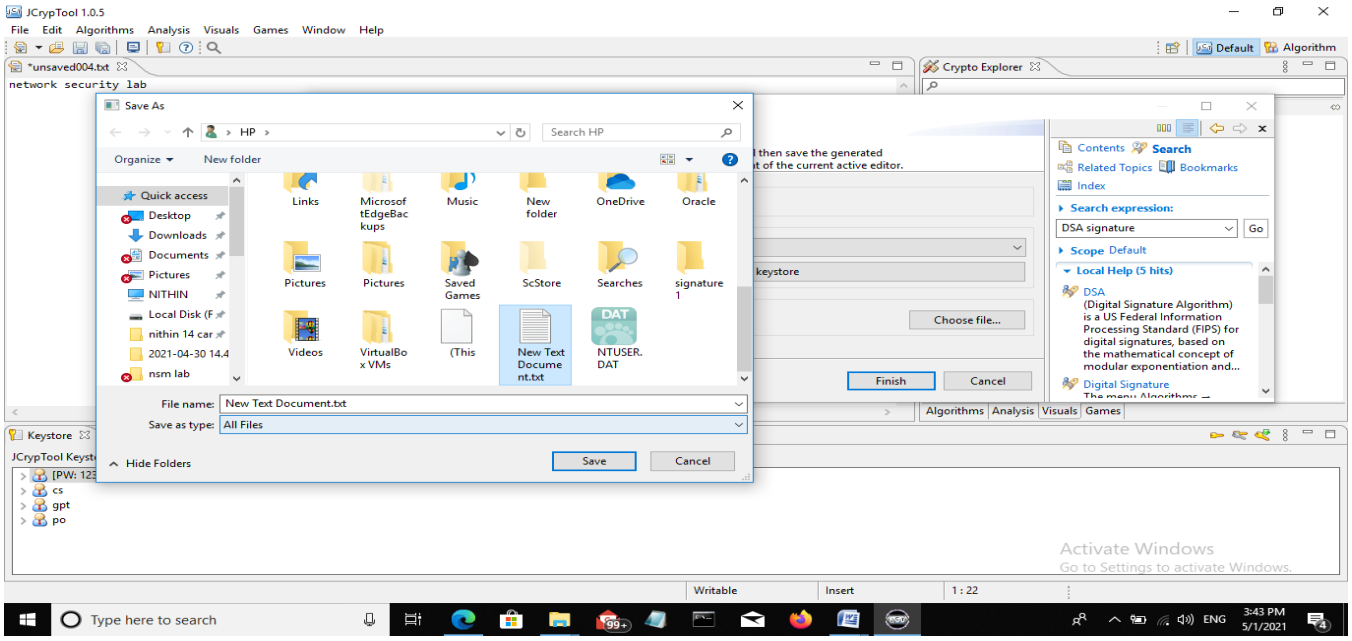

JCrypTool 1.0.5
File Edit Algorithms Analysis Visuals Games Window Help
*unsaved004.txt
out004.bin
out005.bin
AES — encryption
AES
To encrypt or decrypt a message with the AES algorithm, choose a key (just manually entered, or from the key store) and pick a padding and block cipher mode.
Operation
Encrypt
Decrypt
Key source
Custom key
Key from keystore
Keystore
Select key: "[PW: 1234] Alice Whitehead" - secret key - 128 bit
or: Create a new key in the keystore
Mode and padding scheme
Mode: (ECB) Electronic Codebook
Padding: PKCS#5 Padding
Finish
Cancel
Keystore
JCrypTool Keystore
[PW: 1234] Alice Whitehead
cs
gpt
Activate Windows
Go to Settings to activate Windows.
Overwrite
0x2C = 44 = 00101100
0 (0x0) : 32 (0x20)
Type here to search
ENG
3:21 PM
5/1/2021

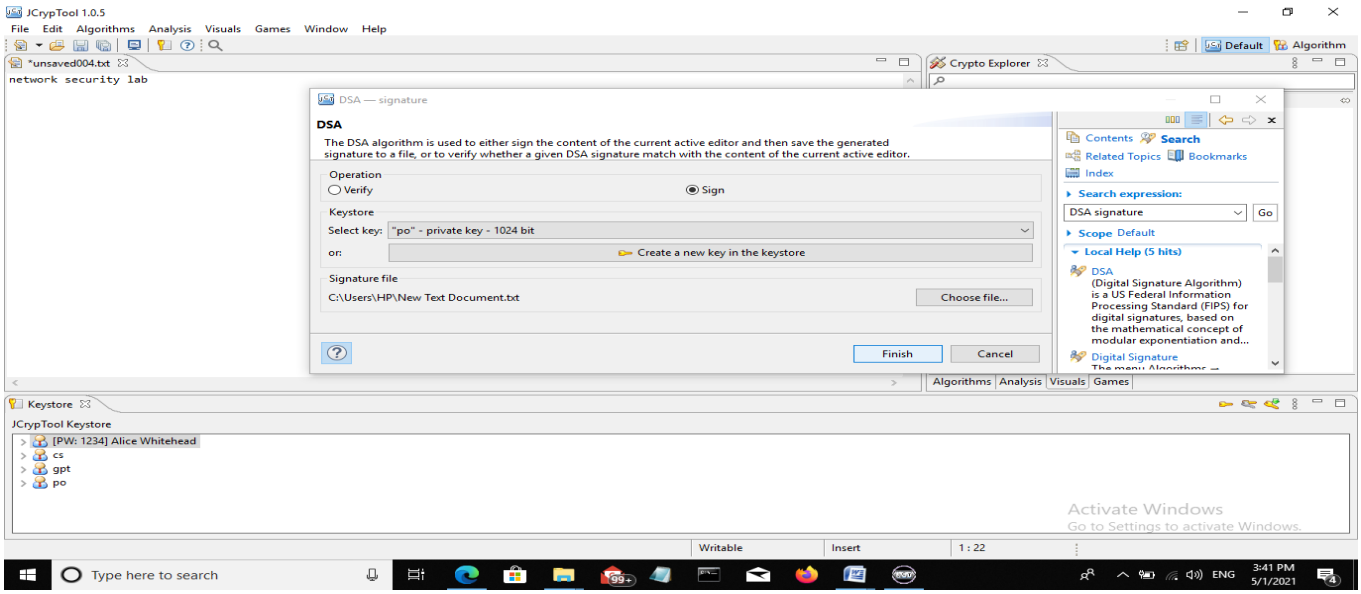

JCrypTool 1.0.5
File Edit Algorithms Analysis Visuals Games Window Help
*unsaved004.txt
out004.bin
out005.bin
Crypto Explorer
Asymmetric
Classic
ADFGVX
Autokey-Vigenère
Bifid
Caesar
Hash
MAC
Random Number Generator
Signature
Symmetric
AES
ARC4/Spritz
Dragon
IDEA
Enter Password
Please enter the key protection password. Keys included in JCrypTool for "Alice Whitehead" have the password "1234".
OK
Cancel
Keystore
JCrypTool Keystore
[PW: 1234] Alice Whitehead
cs
gpt
Activate Windows
Go to Settings to activate Windows.
Overwrite
0x2C = 44 = 00101100
0 (0x0) : 32 (0x20)
Type here to search
ENG
3:20 PM
5/1/2021

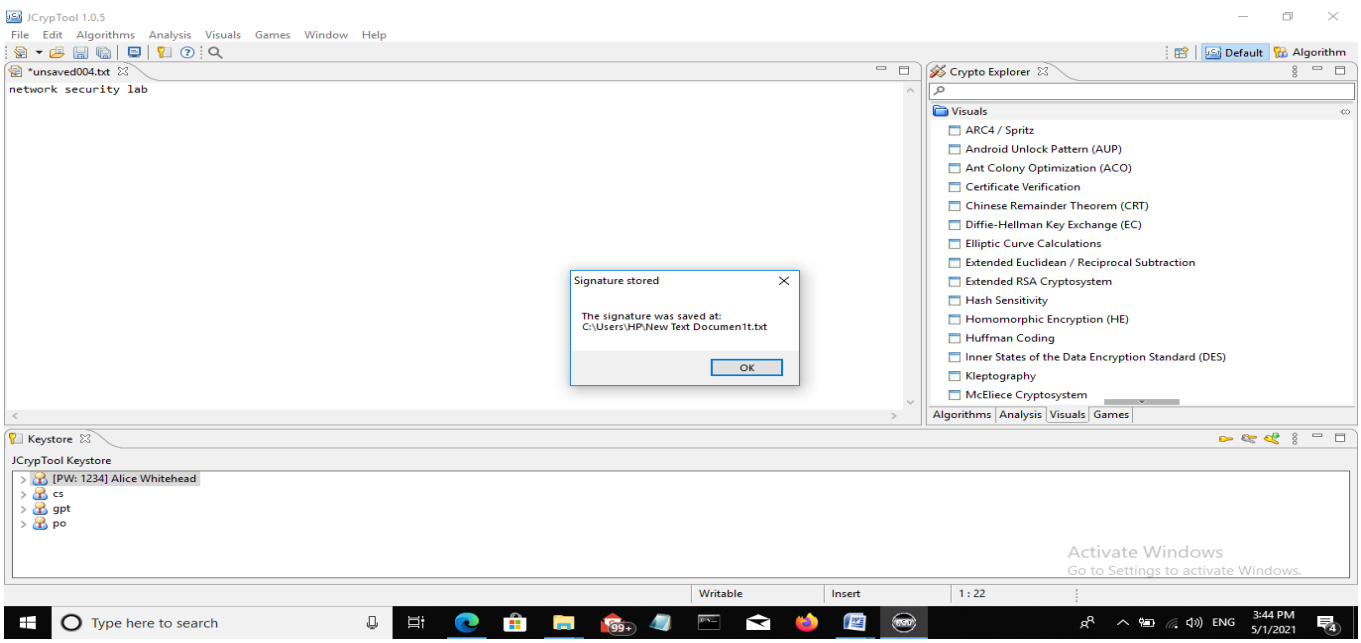


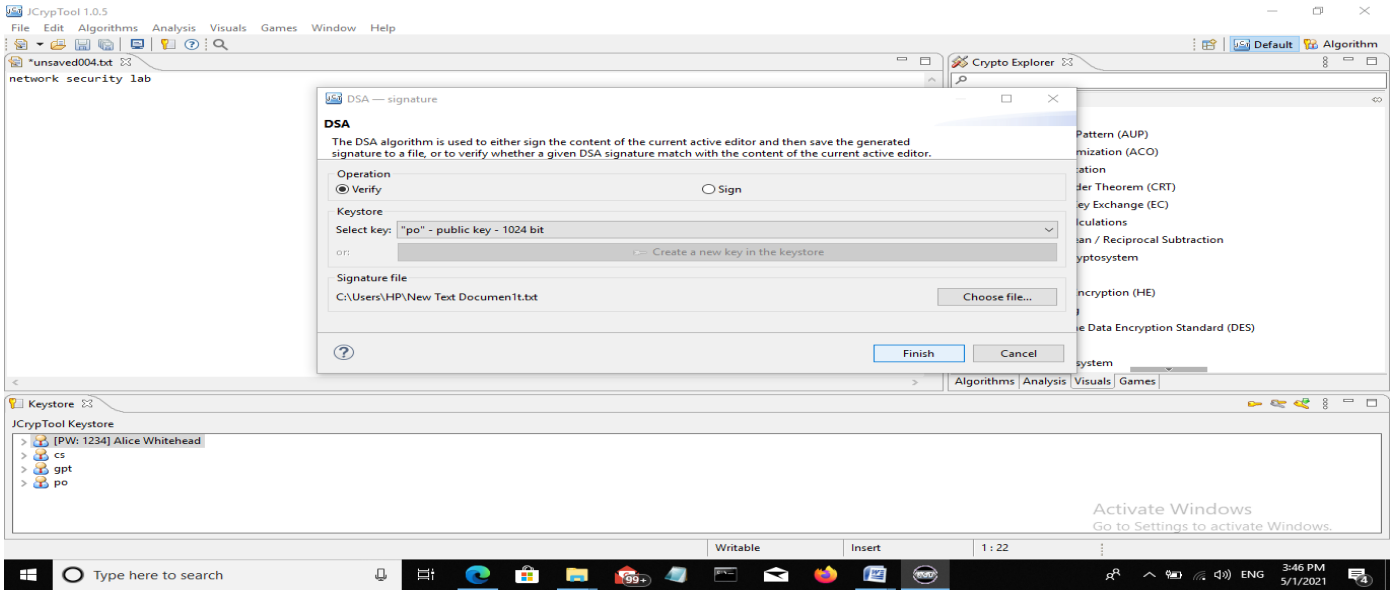
From menu bar select Algorithm-------->Signature--------->DSA and follow steps as in images.

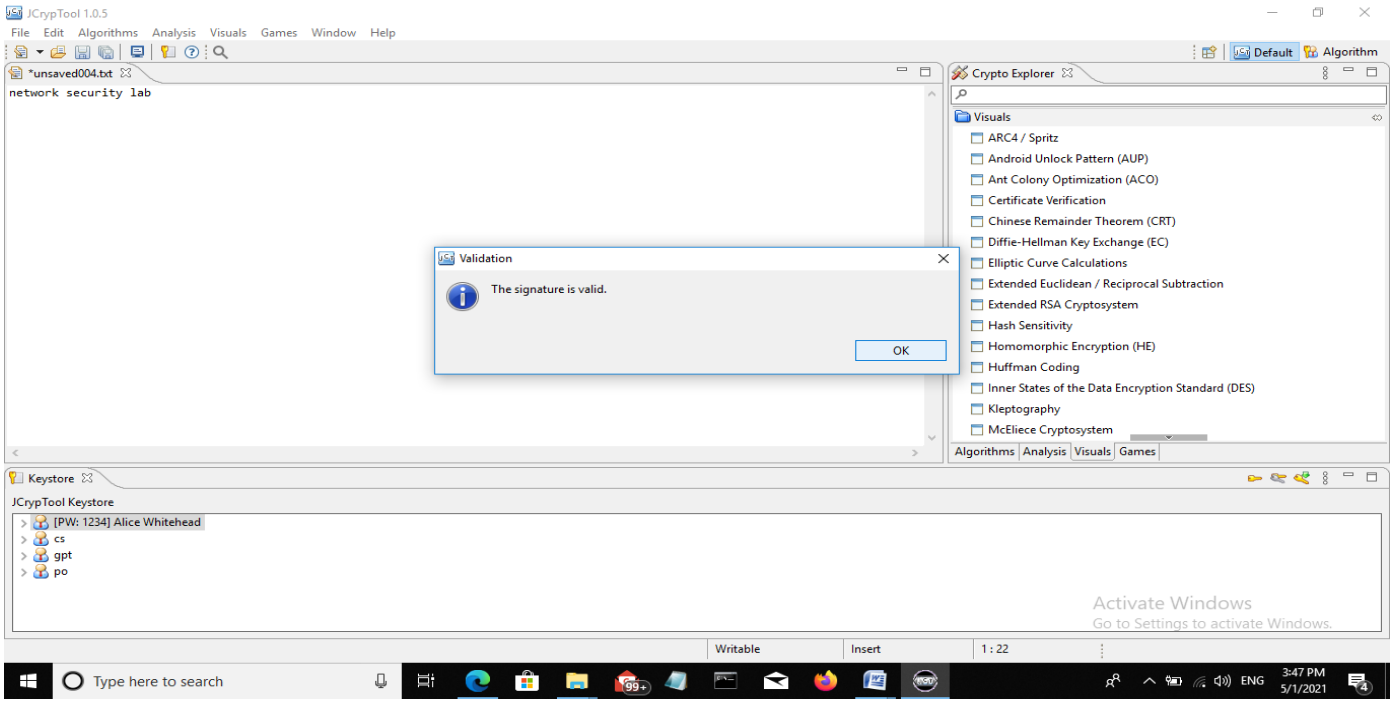



JCrypTool 1.0.5
File Edit Algorithms Analysis Visuals Games Window Help
*unsaved004.txt
network security lab
Save As
HP
Search HP
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
NITHIN
Local Disk (F
nithin 14 car
2021-04-30 14.4
nsm lab
Links
Microsof tEdgeBac kups
Music
New folder
OneDrive
Oracle
Pictures
Pictures
Saved Games
ScStore
Searches
signature 1
Videos
VirtualBo x VMs
(This
New Text Docume nt.txt
NTUSER. DAT
File name: New Text Document.txt
Save as type: All Files
Hide Folders
Save
Cancel
Crypto Explorer
Contents
Search
Related Topics
Bookmarks
Index
Search expression:
DSA signature
Go
Scope Default
Local Help (5 hits)
DSA
(Digital Signature Algorithm) is a US Federal Information Processing Standard (FIPS) for digital signatures, based on the mathematical concept of modular exponentiation and...
Digital Signature
Choose file...
Finish
Cancel
Keystore
JCrypTool Keystore
[PW: 123
cs
gpt
po
Activate Windows
Go to Settings to activate Windows.
Writable
Insert
1 : 22
Type here to search
ENG
3:43 PM
5/1/2021


JCrypTool 1.0.5
File Edit Algorithms Analysis Visuals Games Window Help
*unsaved004.txt
network security lab
DSA — signature
DSA
The DSA algorithm is used to either sign the content of the current active editor and then save the generated signature to a file, or to verify whether a given DSA signature match with the content of the current active editor.
Operation
Verify
Sign
Keystore
Select key: "po" - private key - 1024 bit
or:
Create a new key in the keystore
Signature file
C:\Users\HP\New Text Document.txt
Choose file...
Finish
Cancel
Crypto Explorer
Contents
Search
Related Topics
Bookmarks
Index
Search expression:
DSA signature
Go
Scope Default
Local Help (5 hits)
DSA
(Digital Signature Algorithm) is a US Federal Information Processing Standard (FIPS) for digital signatures, based on the mathematical concept of modular exponentiation and...
Digital Signature
Keystore
JCrypTool Keystore
[PW: 1234] Alice Whitehead
cs
gpt
po
Activate Windows
Go to Settings to activate Windows.
Writable
Insert
1 : 22
Type here to search
ENG
3:41 PM
5/1/2021


JCrypTool 1.0.5
File Edit Algorithms Analysis Visuals Games Window Help
*unsaved004.txt
network security lab
Signature stored
The signature was saved at: C:\Users\HP\New Text Documen1t.txt
OK
Crypto Explorer
Visuals
ARC4 / Spritz
Android Unlock Pattern (AUP)
Ant Colony Optimization (ACO)
Certificate Verification
Chinese Remainder Theorem (CRT)
Diffie-Hellman Key Exchange (EC)
Elliptic Curve Calculations
Extended Euclidean / Reciprocal Subtraction
Extended RSA Cryptosystem
Hash Sensitivity
Homomorphic Encryption (HE)
Huffman Coding
Inner States of the Data Encryption Standard (DES)
Kleptography
McEliece Cryptosystem
Keystore
JCrypTool Keystore
[PW: 1234] Alice Whitehead
cs
gpt
po
Activate Windows
Go to Settings to activate Windows.
Writable
Insert
1 : 22
Type here to search
ENG
3:44 PM
5/1/2021


JCrypTool 1.0.5
File Edit Algorithms Analysis Visuals Games Window Help
*unsaved004.txt
network security lab
DSA — signature
DSA
The DSA algorithm is used to either sign the content of the current active editor and then save the generated signature to a file, or to verify whether a given DSA signature match with the content of the current active editor.
Operation
Verify
Sign
Keystore
Select key: "po" - public key - 1024 bit
or: Create a new key in the keystore
Signature file
C:\Users\HP\New Text Documen1t.txt
Choose file...
Finish
Cancel
Crypto Explorer
Default
Algorithm
Algorithms Analysis Visuals Games
Keystore
JCrypTool Keystore
[PW: 1234] Alice Whitehead
cs
gpt
po
Activate Windows
Go to Settings to activate Windows.
Writable
Insert
1 : 22
Type here to search
ENG
3:46 PM
5/1/2021

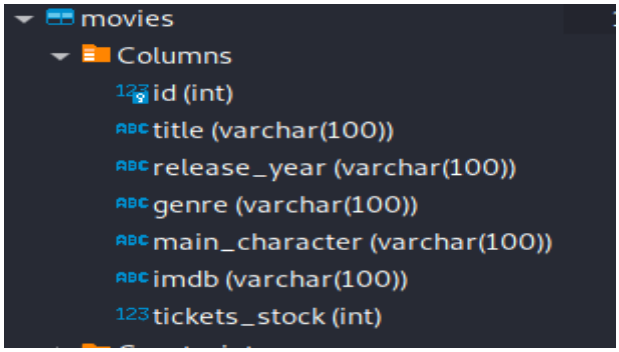

JCrypTool 1.0.5
File Edit Algorithms Analysis Visuals Games Window Help
*unsaved004.txt
network security lab
Validation
The signature is valid.
OK
Crypto Explorer
Default
Algorithm
Visuals
ARC4 / Spritz
Android Unlock Pattern (AUP)
Ant Colony Optimization (ACO)
Certificate Verification
Chinese Remainder Theorem (CRT)
Diffie-Hellman Key Exchange (EC)
Elliptic Curve Calculations
Extended Euclidean / Reciprocal Subtraction
Extended RSA Cryptosystem
Hash Sensitivity
Homomorphic Encryption (HE)
Huffman Coding
Inner States of the Data Encryption Standard (DES)
Kleptography
McEliece Cryptosystem
Algorithms Analysis Visuals Games
Keystore
JCrypTool Keystore
[PW: 1234] Alice Whitehead
cs
gpt
po
Activate Windows
Go to Settings to activate Windows.
Writable
Insert
1 : 22
Type here to search
ENG
3:47 PM
5/1/2021

BWAPP SQL INJECTION GET/SEARCH


```
<?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



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

- 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

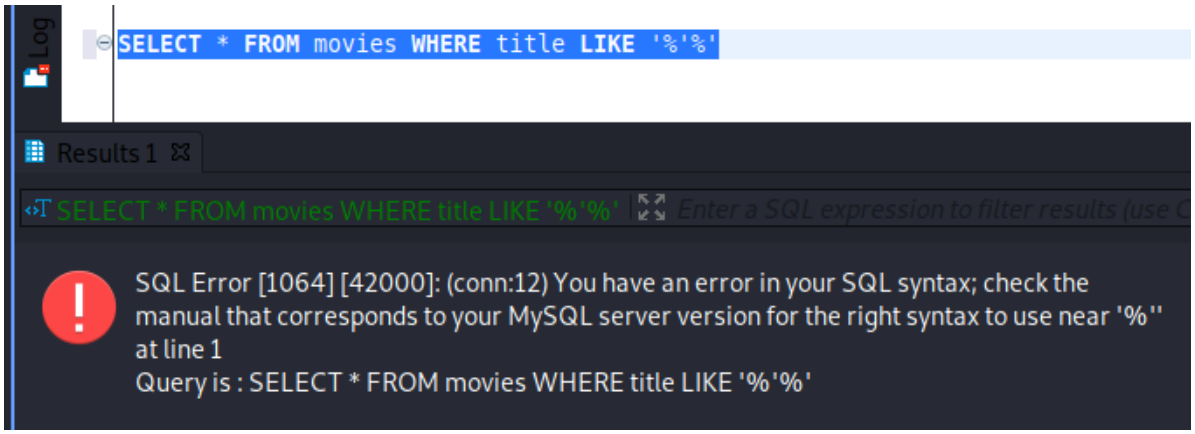
Initial code

SELECT * FROM movies WHERE title LIKE ‘%” . sqli($title) . “%’

After user input

SELECT * FROM movies WHERE title LIKE ‘%’%’

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



- 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

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

movies 1

SELECT * FROM movies WHERE title LIKE '%'

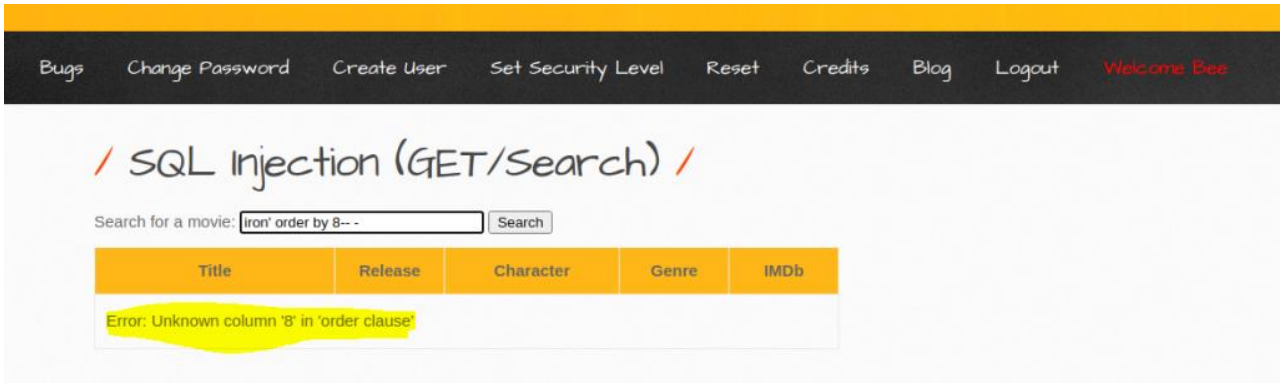
	id	title	release_year	genre	main_character	imdb	tickets_stock
1	1	G.I. Joe: Retaliation	2013	action	Cobra Commander	tt1583421	100
2	2	Iron Man	2008	action	Tony Stark	tt0371746	53
3	3	Man of Steel	2013	action	Clark Kent	tt0770828	78
4	4	Terminator Salvation	2009	sci-fi	John Connor	tt0438488	100
5	5	The 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

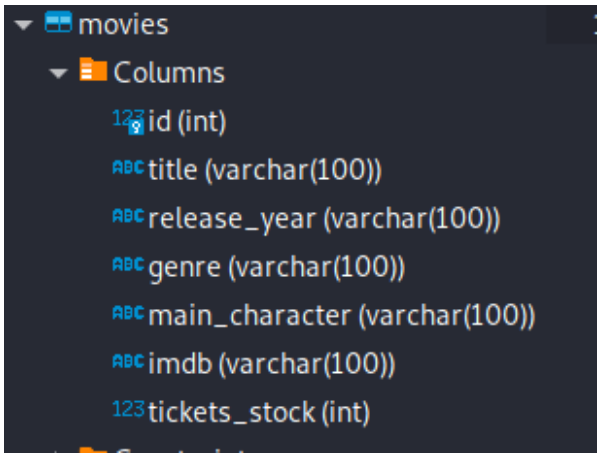
We are going to do exploitation to this vulnerability code by using **union select**. Why I choose union select because this page allows us to get the data. The first thing to do with the union-based attack is to identify the number of columns affected by the query because union select requires having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



- 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– –

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– –

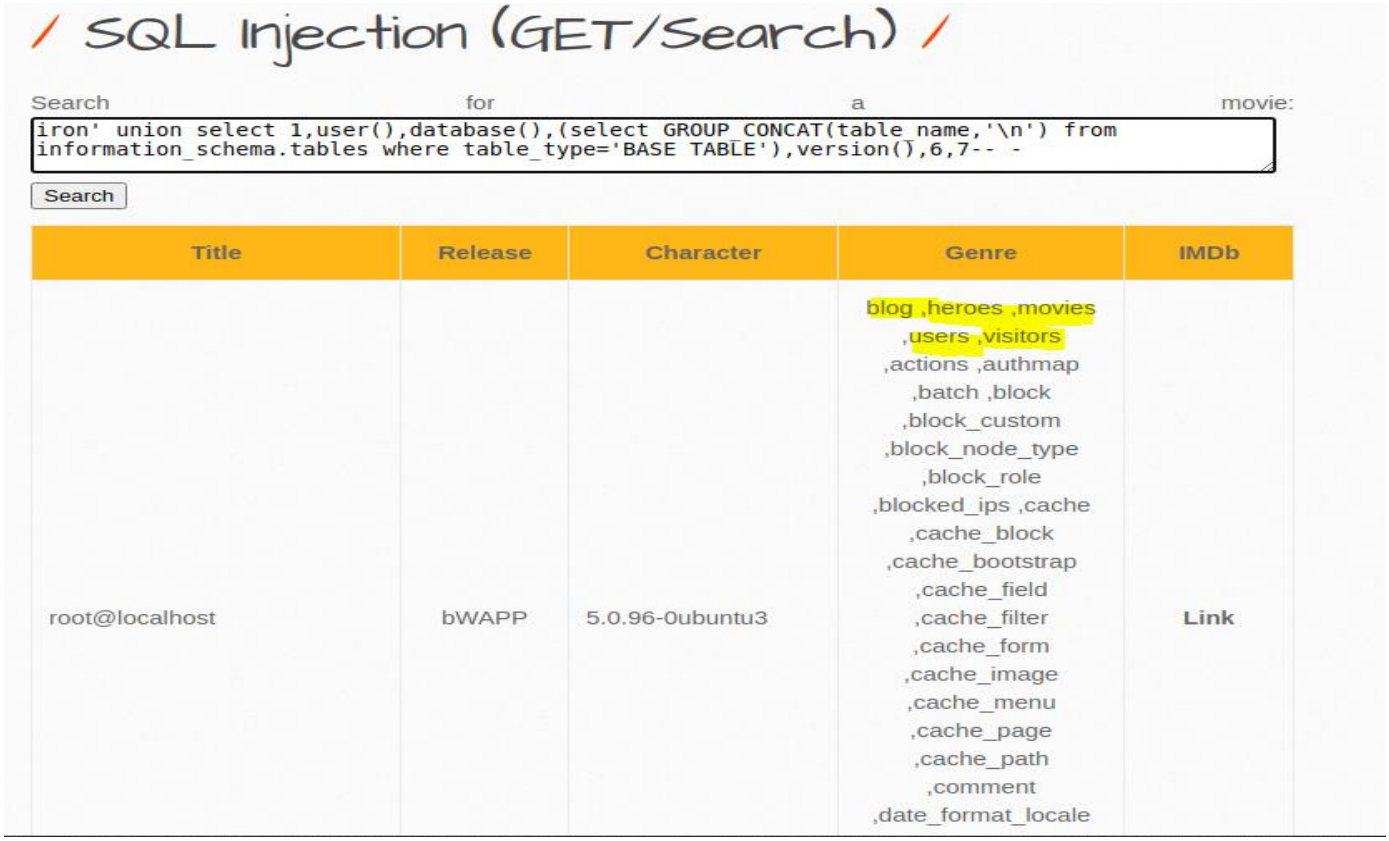
The complete query will become like this SELECT * FROM movies WHERE title LIKE '%iron' union select 1,2,3,4,5,6,7– – %'

Below are queries to go further

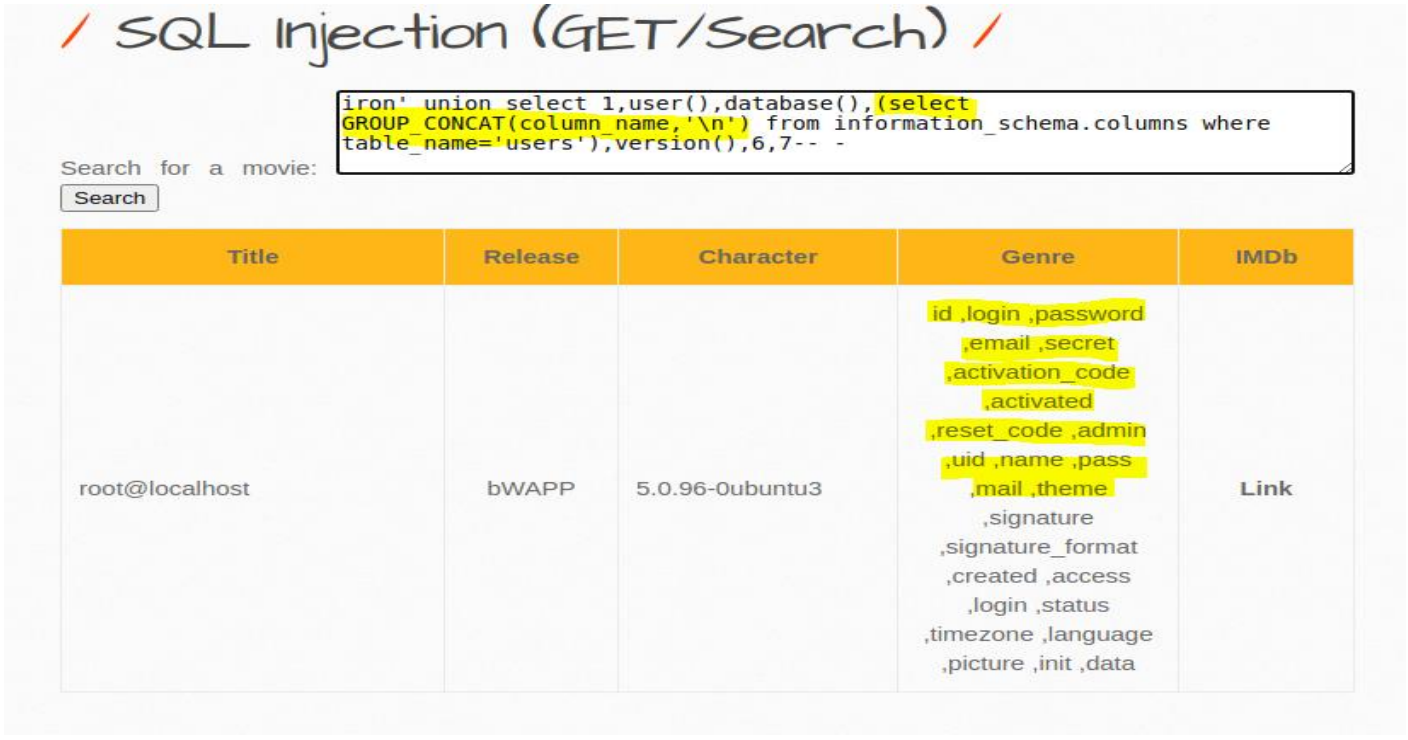
Getting user of the database

Getting name of the database

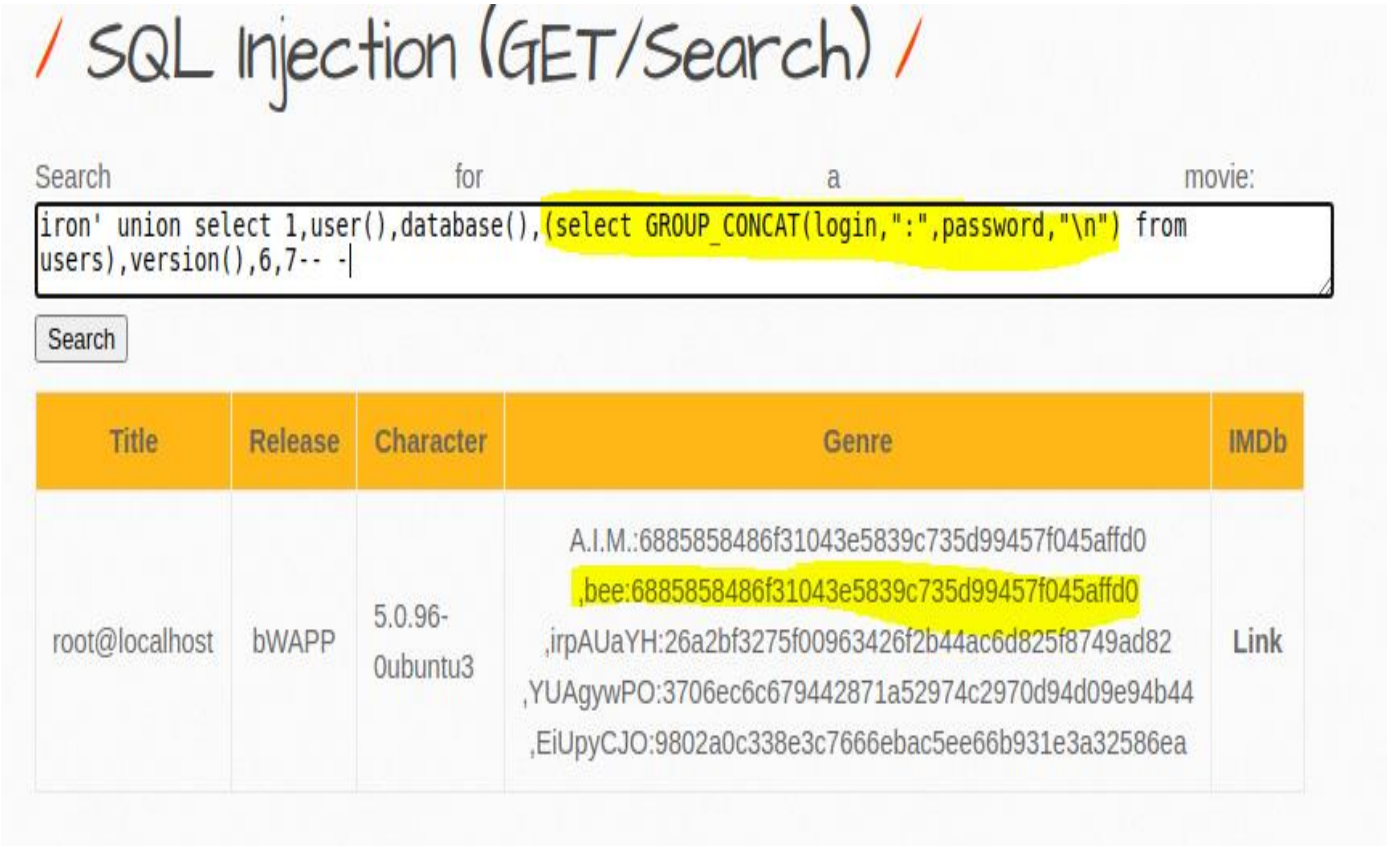
Getting the tables name of the database



Getting the users table column name



Extracting value from table users



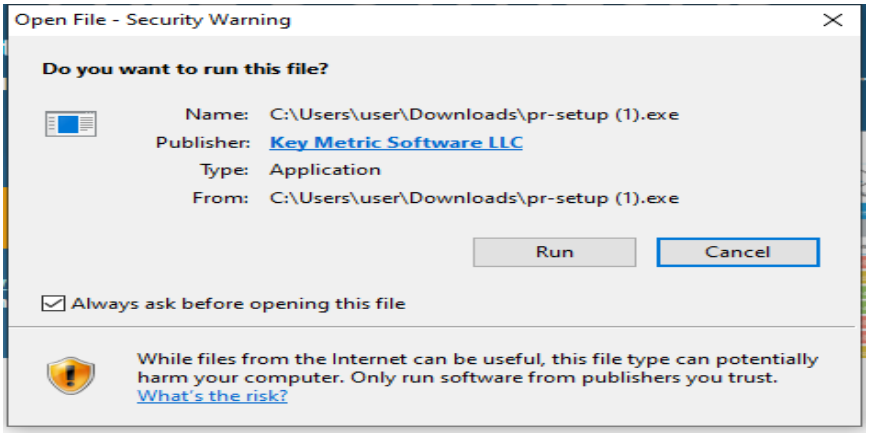
Demonstrate NTFS file system using NTFS permission reporter.

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

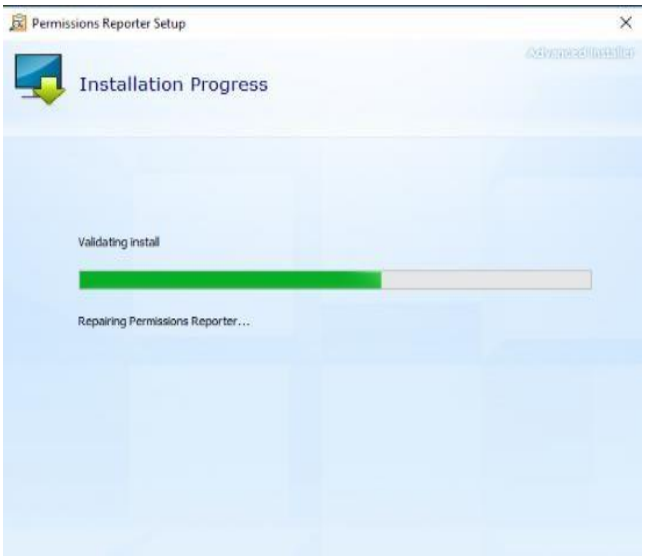
- **Step 2**: Click on Download Now

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

- **Step 4**: Click Run



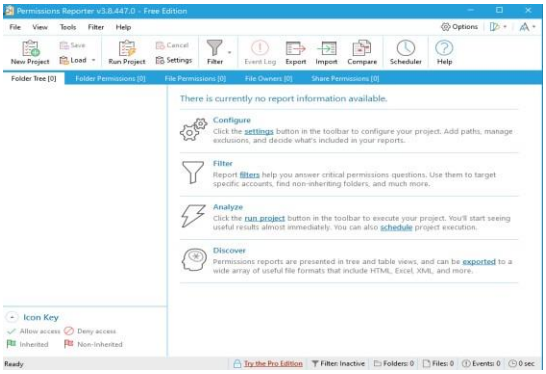
- **Step 5:** Click on Next



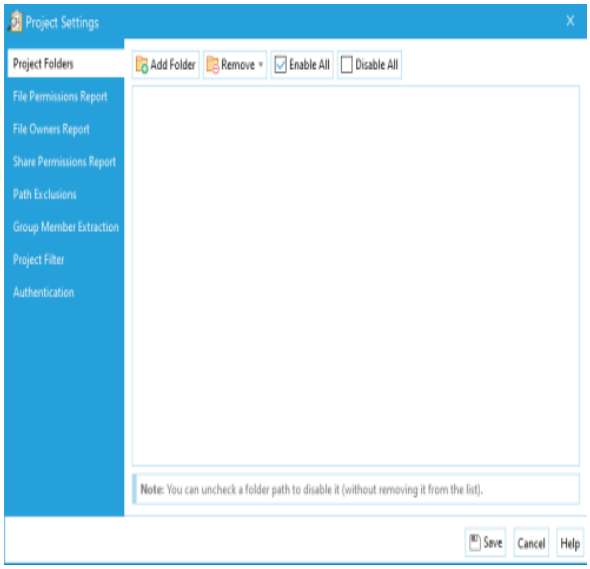
- **Step 6**: Click on Close

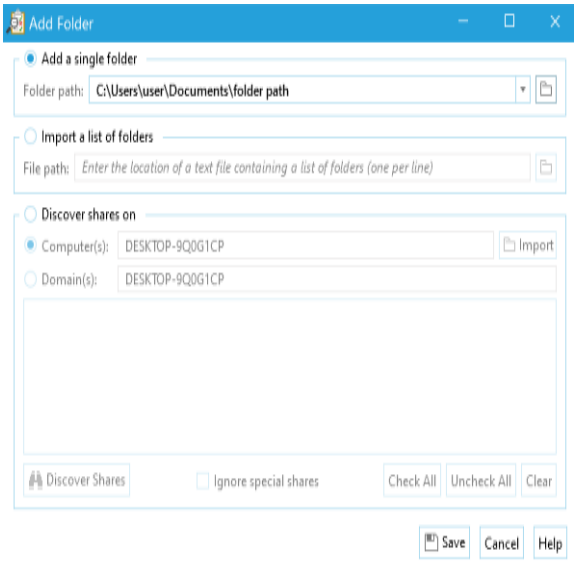
- **Step 7**: open the permission reporter

- **Step 8:** In Configure, Click on settings

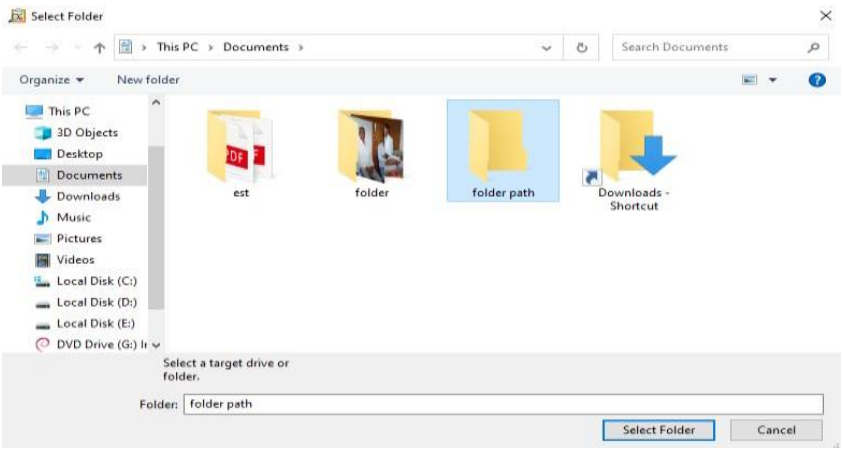


- **Step 9:** In project settings, Select Add Folder

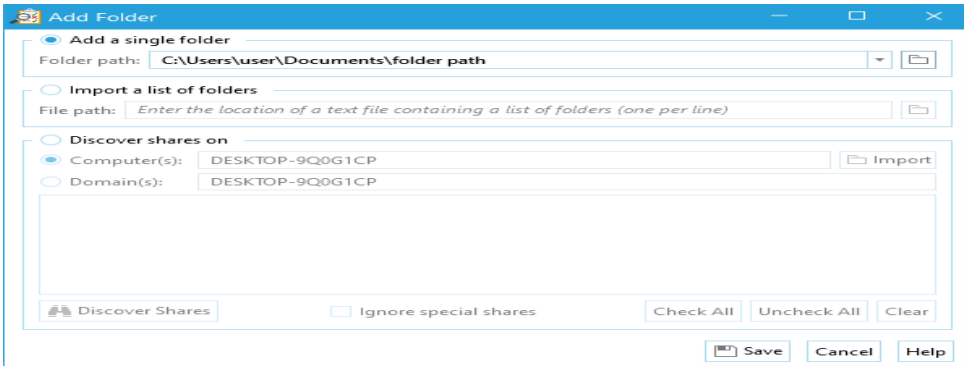




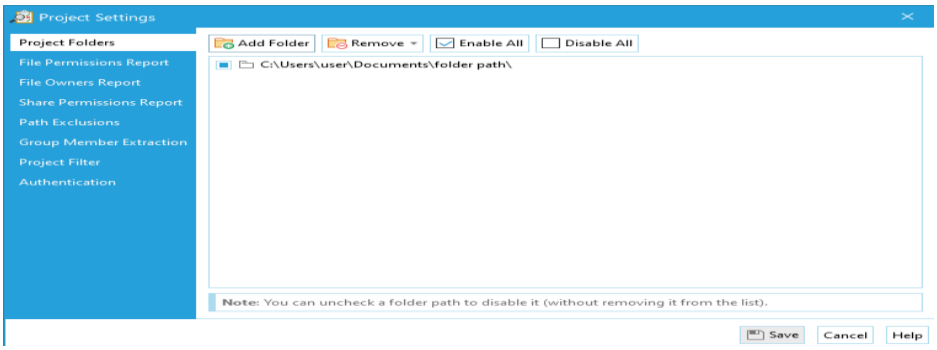
- **Step 10:** Select the folder and Click on Select Folder



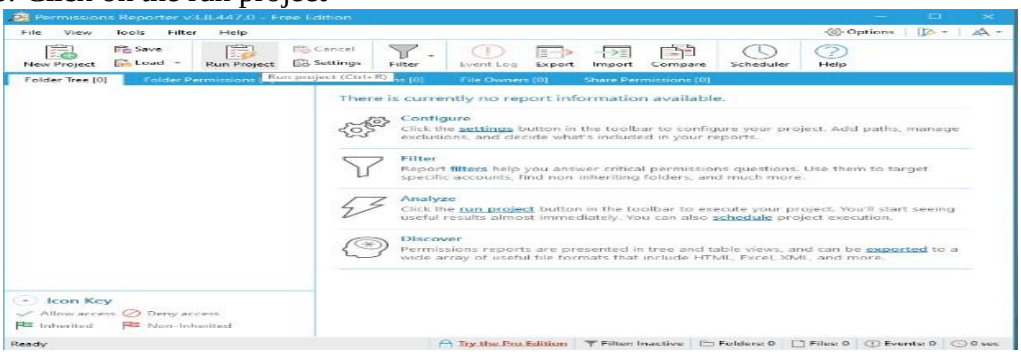
- **Step 11:** Click on Save



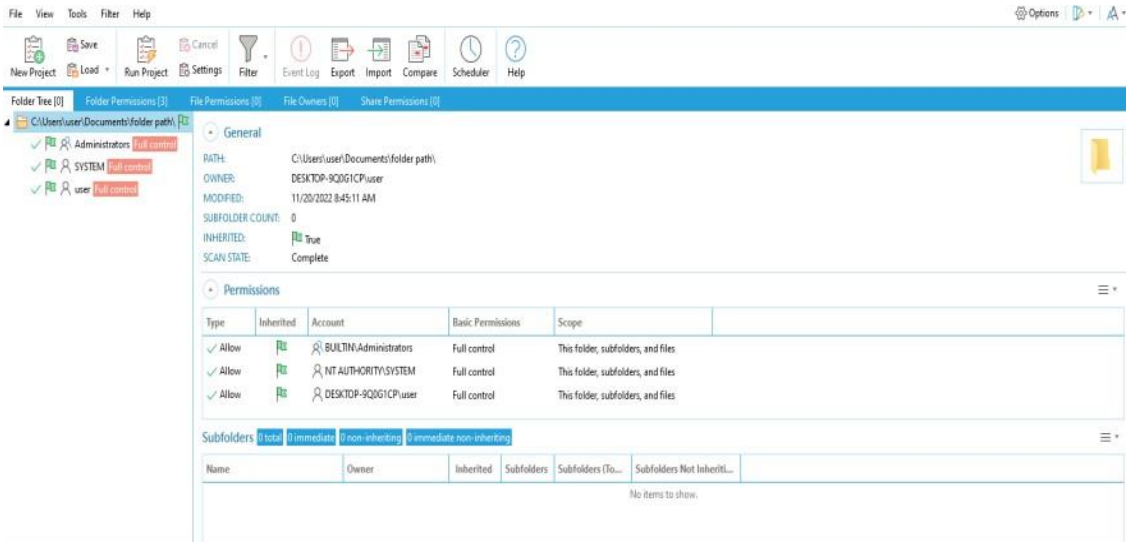
➢ **Step 12:** Click on Save



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

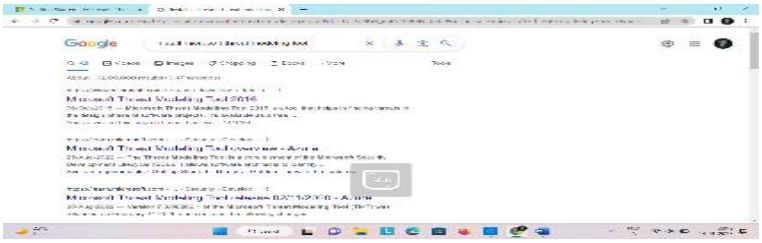


➢ **Step 14** : permission of the select folder display on the screen



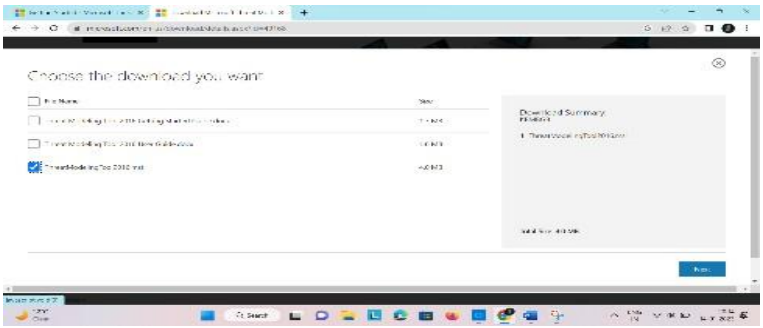
Using the Microsoft threat model software, create a threat model for any application architecture.

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



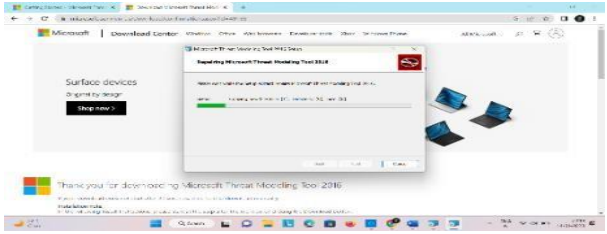
- **Step2** Display the screen Download Microsoft threat Modeling tool 2016

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



- **Step 4** Click Next

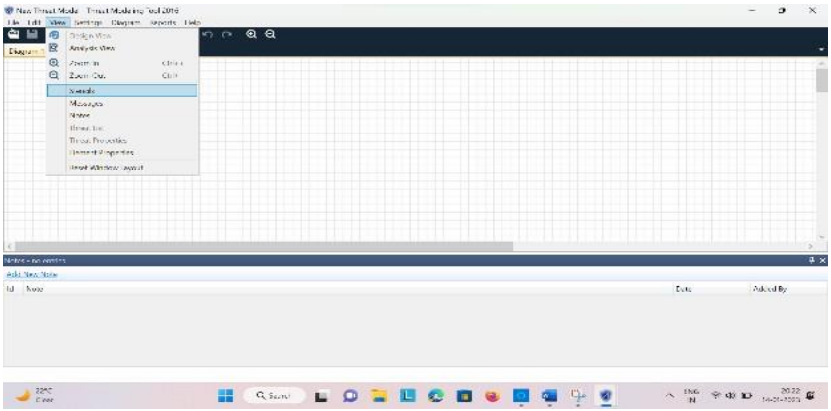
- **Step 5** finish the installation click next step



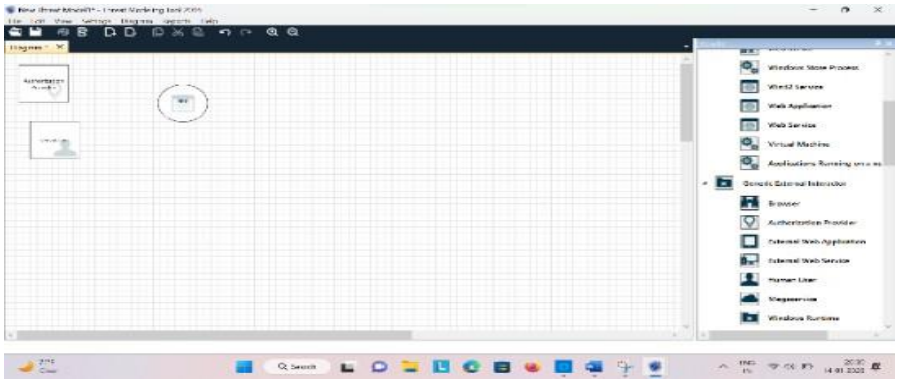
- **Step 6** After installation completed go to Threat Model create A Model

Create application

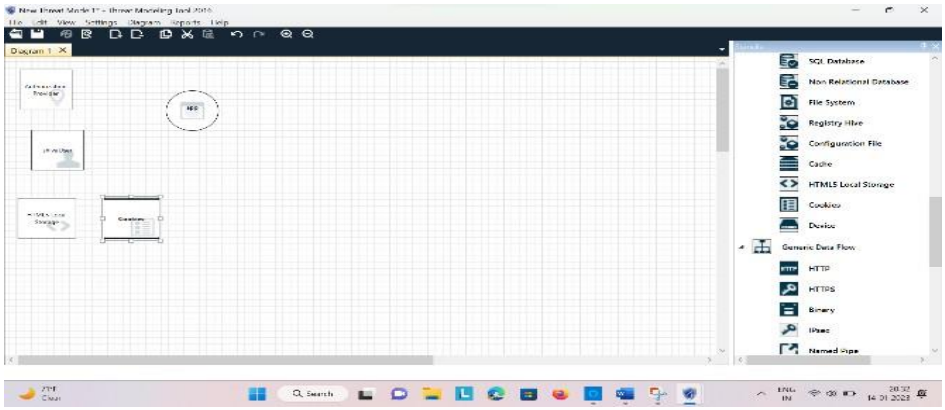
- **Step 7** go to view click stencils display the tools



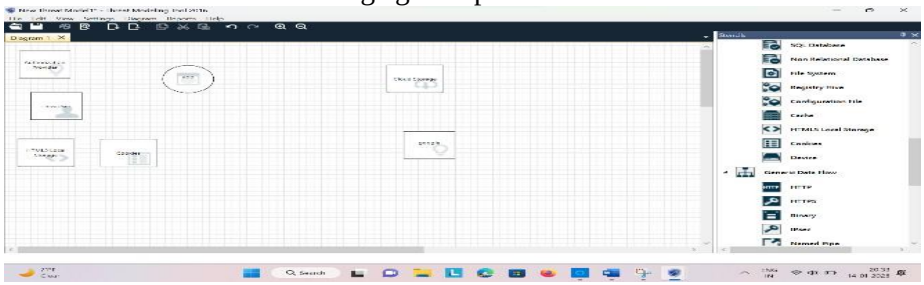
- **Step 8** Take application, Human user, Authentication provider and give the permission



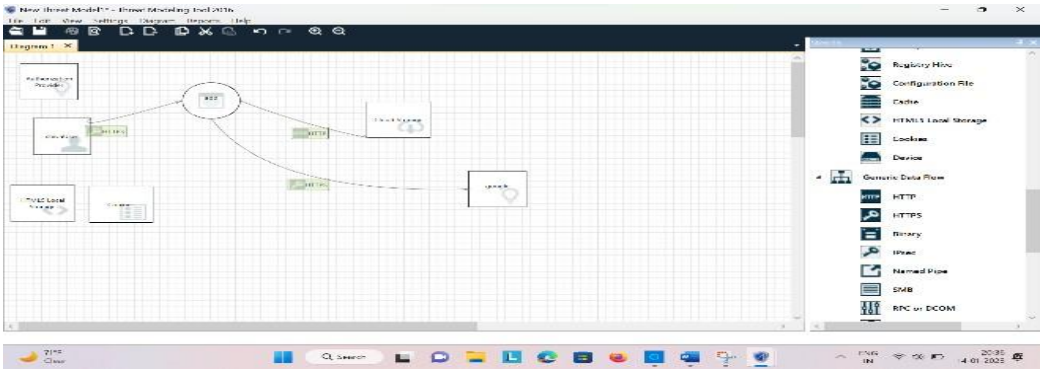
- **Step 9** Take local storage HTML and security cookies



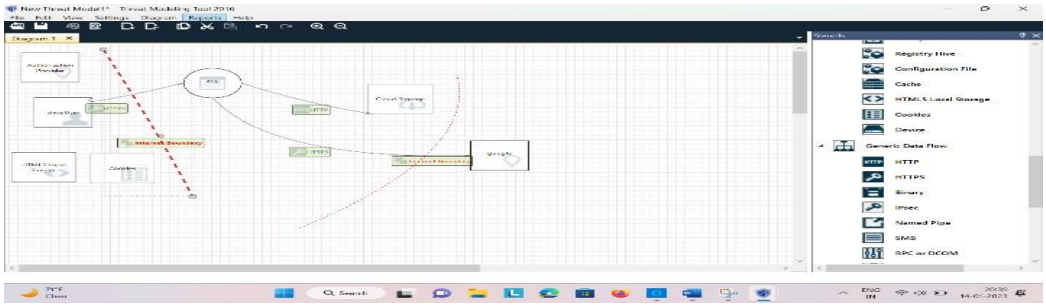
- **Step 10** Take browser and cloud storage give a permission



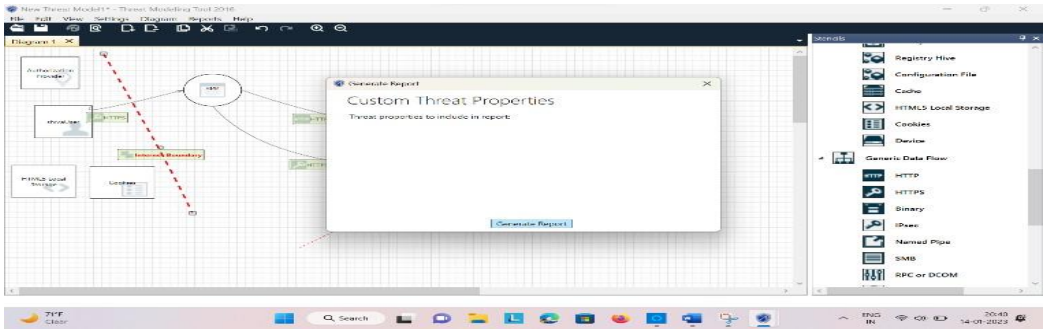
- **Step 11** Assign HTTPS user, google to app and HTTP app to storage



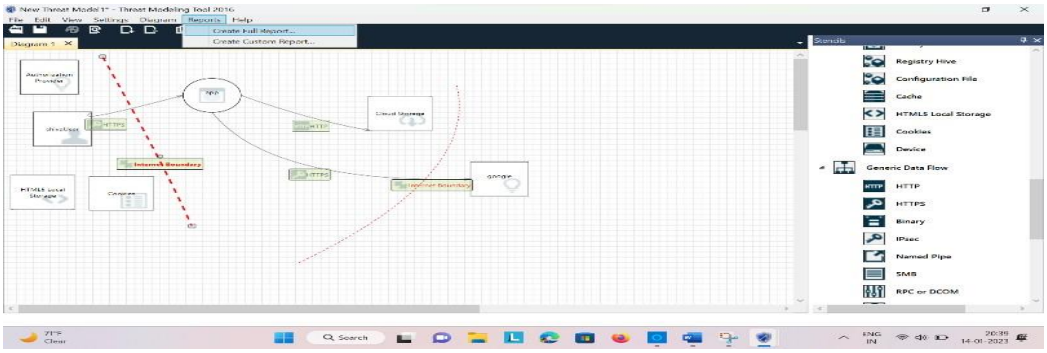
- **Step 12** Add Internet Boundary and got reports



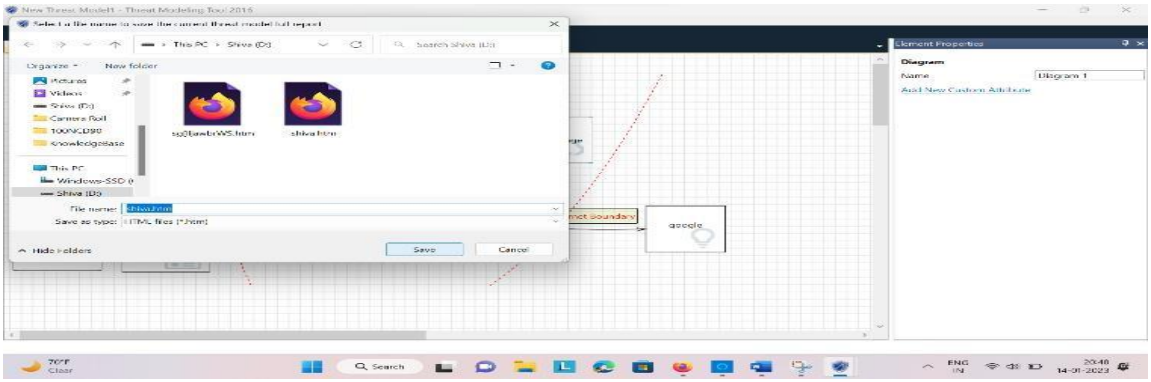
- **Step 13** Click Create Full Report



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



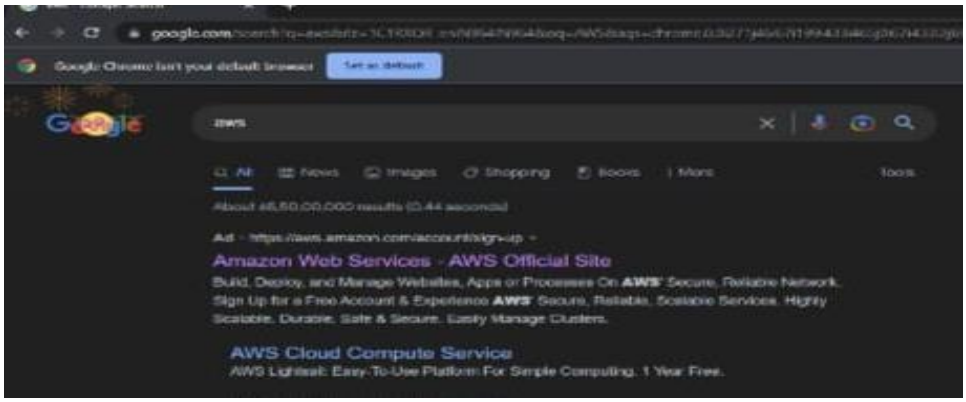
- **Step 15** Save the file and view the report



- **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 onverify email address

Step 4: - Enter verification code then click on verify

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

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

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

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

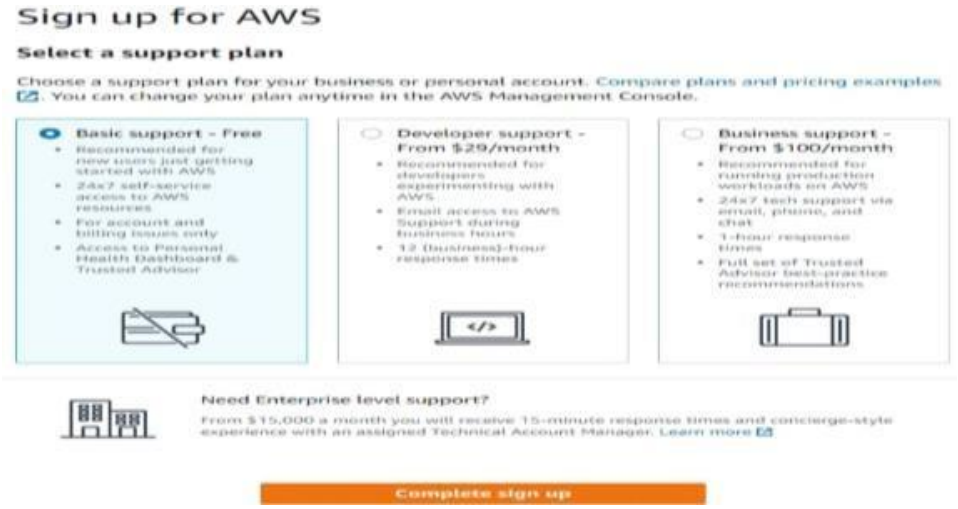
- **Step 9: -** Enter your phone number & captcha then click on send SMS

- Step 10: - Then enter the verification code

qq

q

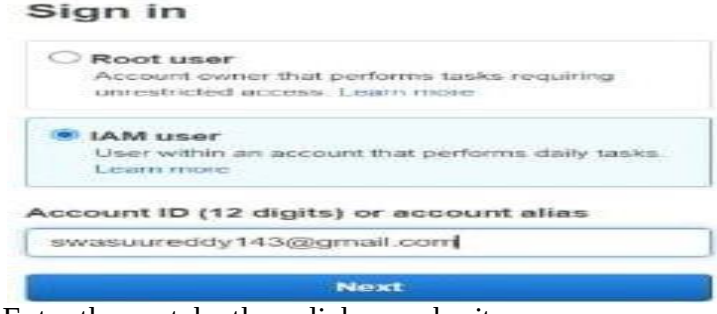
- Step 11: - Then click on complete sign up



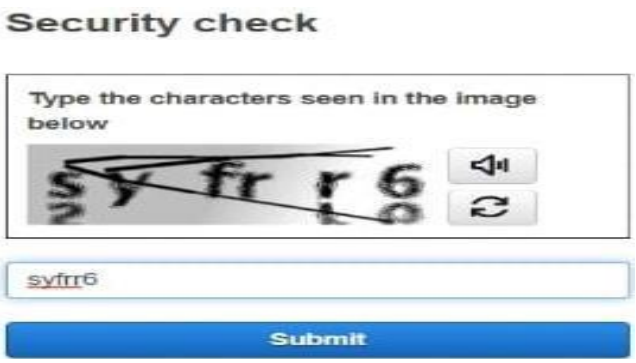
- Step 12: - Click on Go to AWS management console

- 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



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

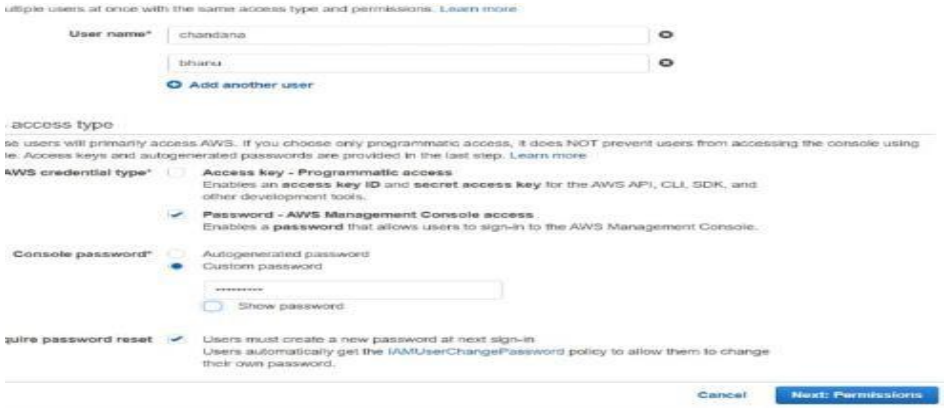
- Step 17: - Then click on IAM
- Step 18: - Click on user

- Step 19: - Then click on Add user

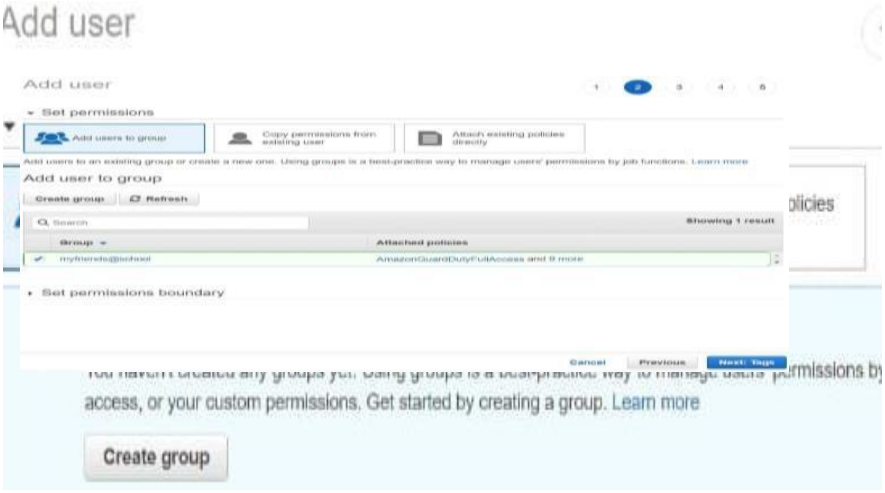
- Step 20: - Enter user name then if you want add multiple user

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

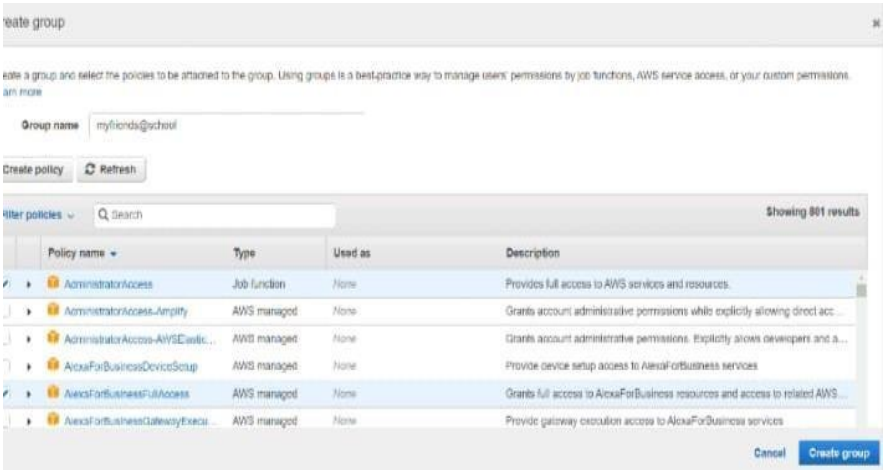
  Select the password – AWS MCA. Then Select the customer password& enter the Password. Then click on Next: permission



- Step 21: - Click on create group

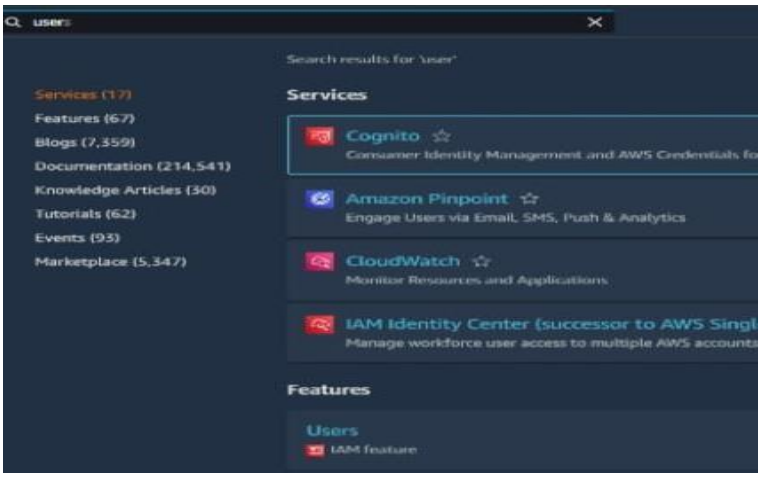


- Step 22: - Enter the group name & Give a policies then click on create group



- 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

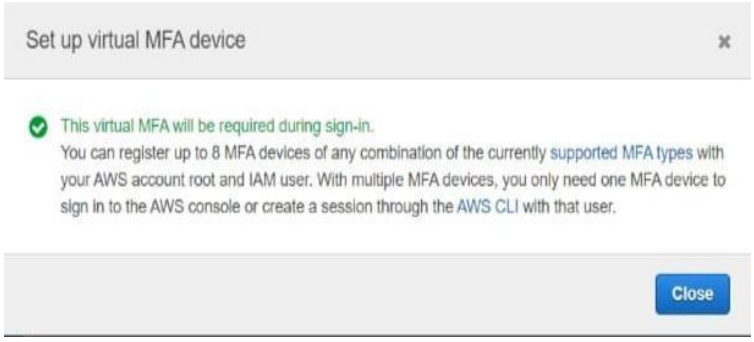
  theAuthenticator app

- 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”



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