

EXPT.No. 1	Explore Compare It Tool to Compare of two files for ForensicInvestigation.	DATE:
-------------------	---	--------------

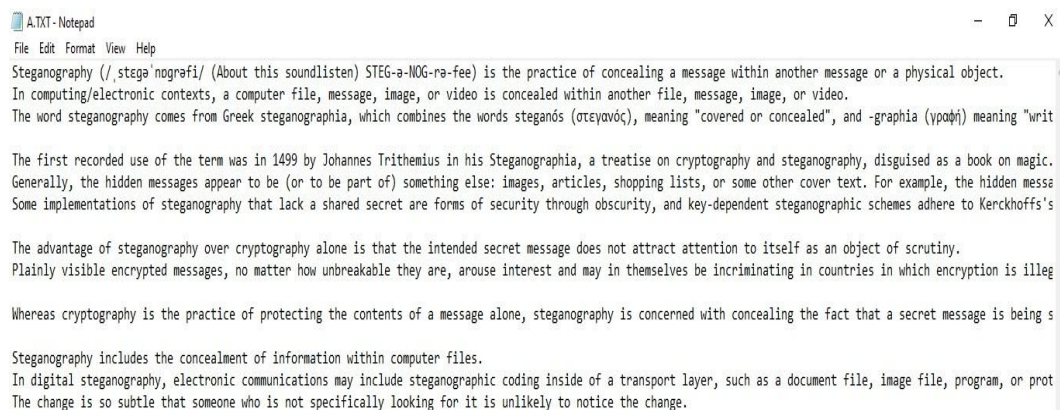
AIM:

The main aim is to comparison of two files for forensics investigation by COMPARE IT tool

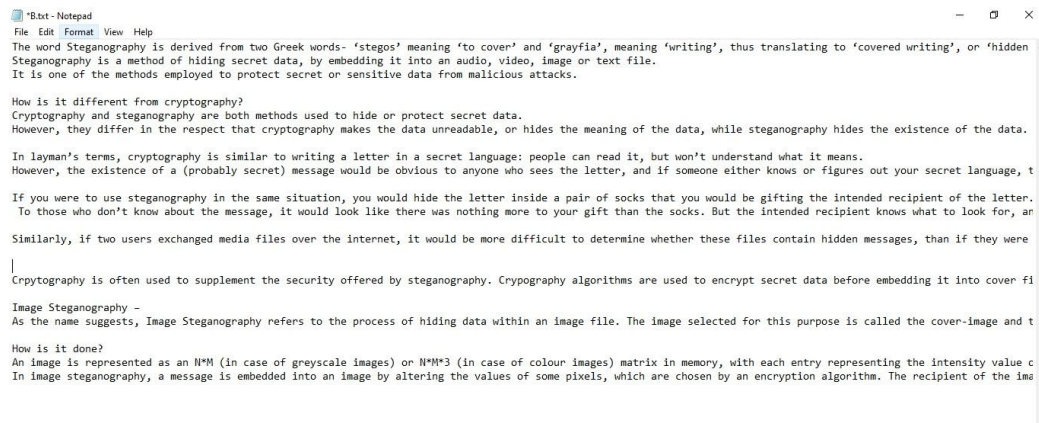
PROCEDURE:

- COMPARE IT is software that displays 2 files side by side, with colored differences sections to simplify analyzing. You can move changes between files with a single mouse click or keystroke, and of course, you have the ability to edit files directly in comparison window.
- It can make colored printout of differences report, exactly as it's on the screen. Firstof all, install the Compare It from the Link given below.
<http://www.grigsoft.com/wincmp3.htm> it is a 1.7 Mb Software package Click on Compare It Tool, It will show a window to select the files to be compared.
- First, select the first file and click on open and then select the second file and click on open.

STEP 1: open the notepad and create a first text file with the extension .txt and savewith a file name

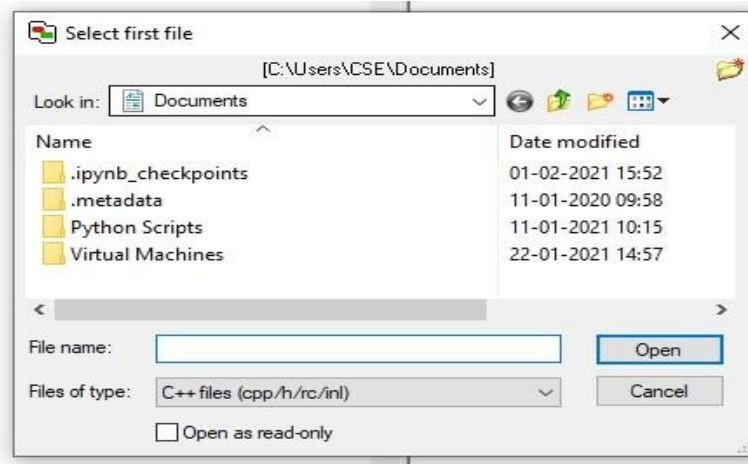


Step 2: create a second text file with the extension .txt

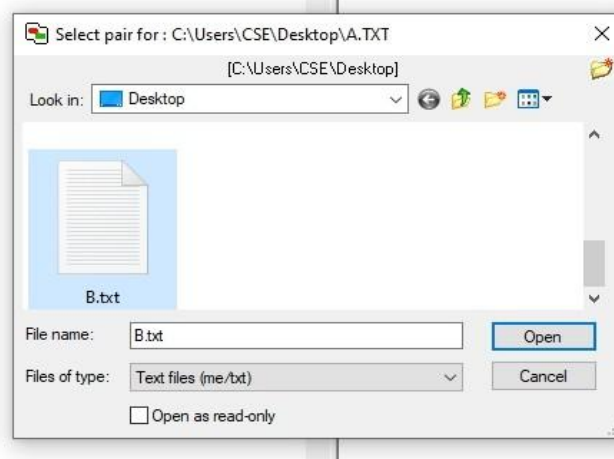


Step 3: Download the compare it tool install the Compare It from the Link given below.
<http://www.grigsoft.com/wincmp3.htm> it is a 1.7 Mb Software package Click on Compare It Tool, It will show a window to select the files to be compared.

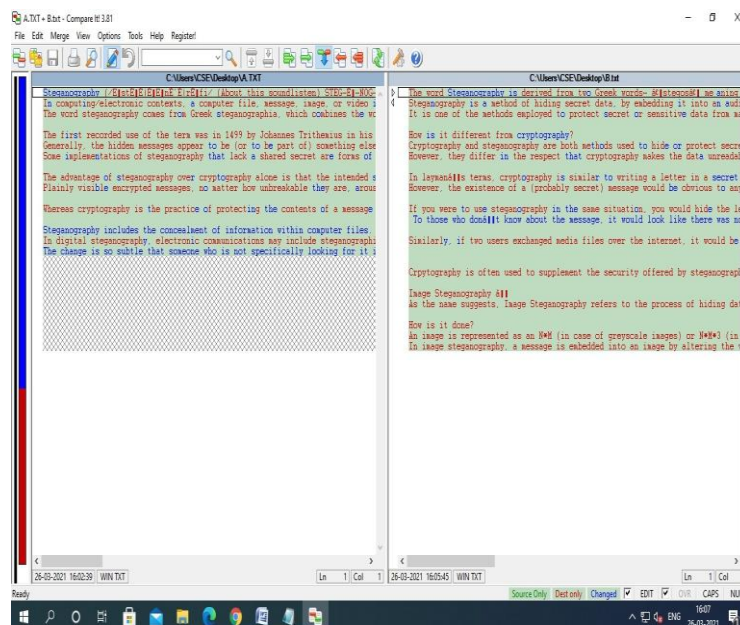
Step 4: Upload the first file to the compare it tool



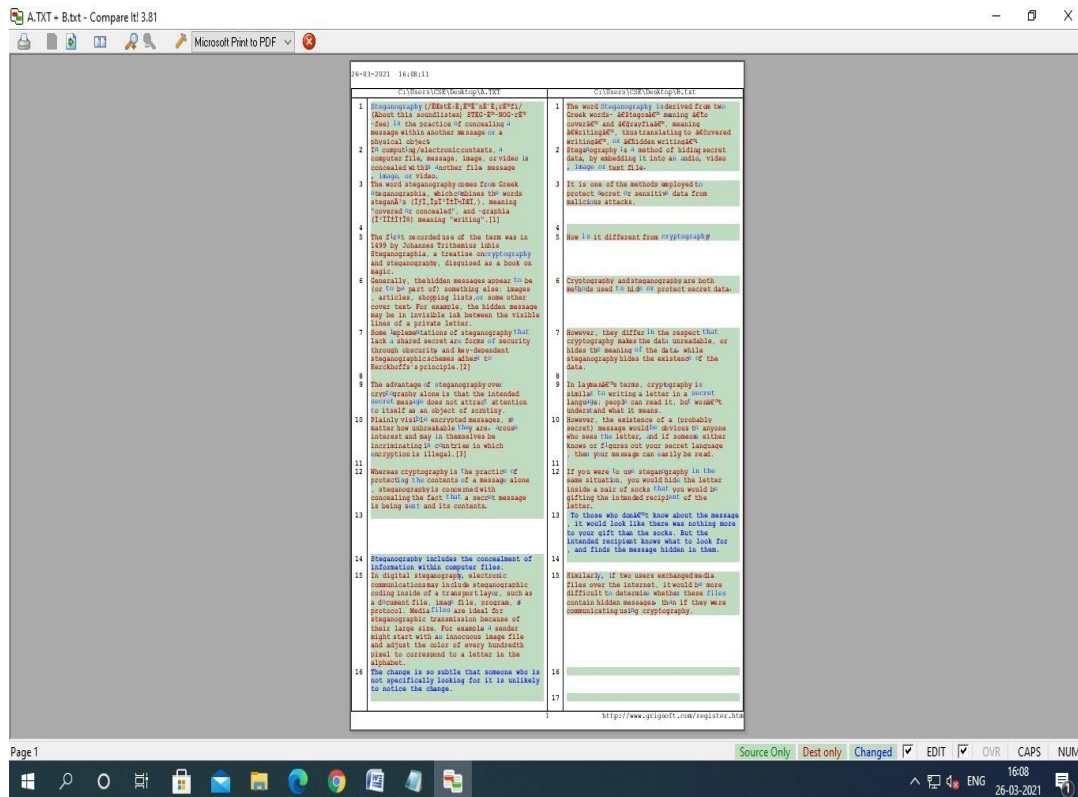
Step 5: upload the second file to the compare it tool



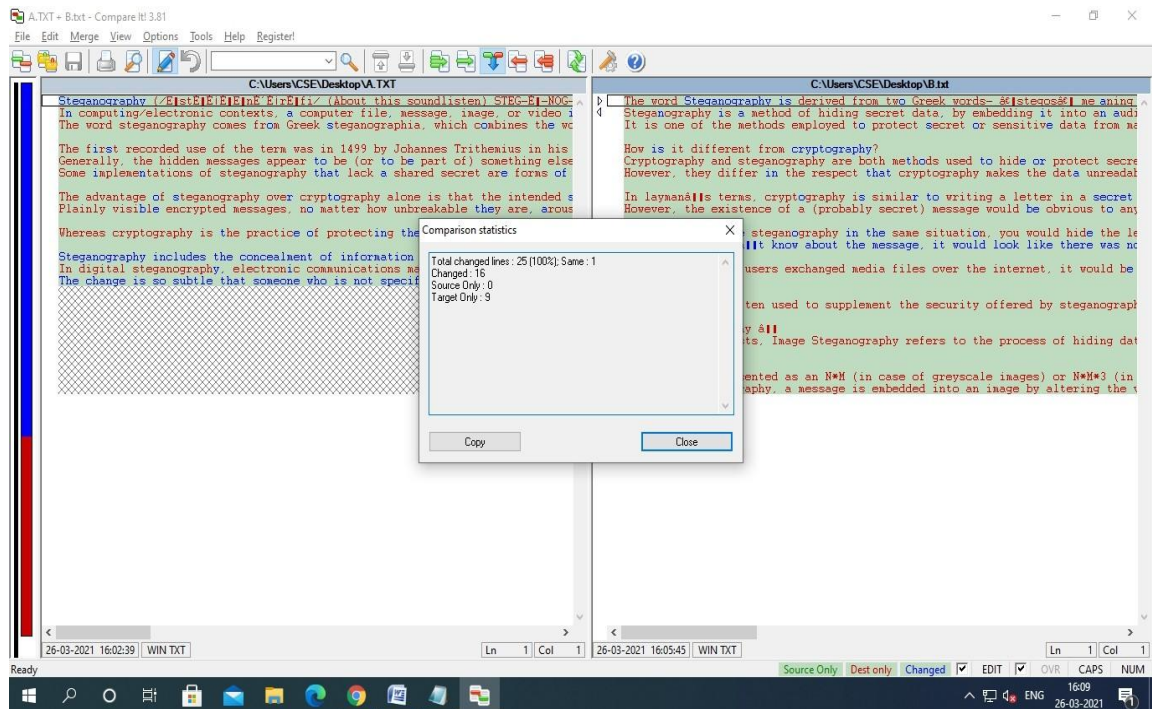
Step 6: Displays 2 files side by side, with colored differences sections to simplify analyzing. You can move changes between files with a single mouse click or keystroke



STEP 7: It also gives you Print report of the difference in the file as follows



STEP 8: the comparison result is get display.



RESULT:

The main aim is to comparison of two files for forensics investigation byCOMPARE IT tool is executed successfully.

EXPT.No. 2	Explore the Snow Tool for hiding the information inText File	DATE:
-------------------	---	--------------

AIM:

The main aim is to hide the information in the Text File Using SNOW TOOL- TextStenography

PROCEDURE:

- 1) Create a text File with some data in the same directory where SNOW Tool is installed.
- 2) In our Experiment Snow tool is installed in Desktop.

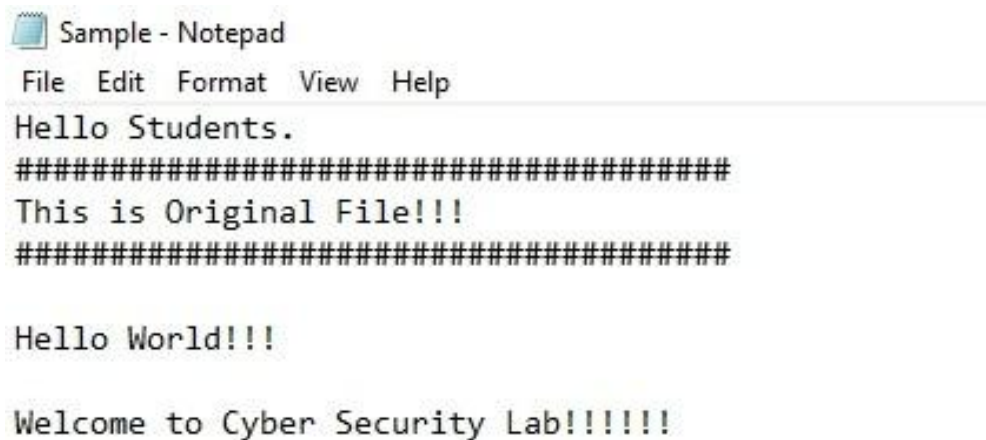


Figure: Text File

- 3) Go to the Command Prompt, Change the directory to run snow Tool

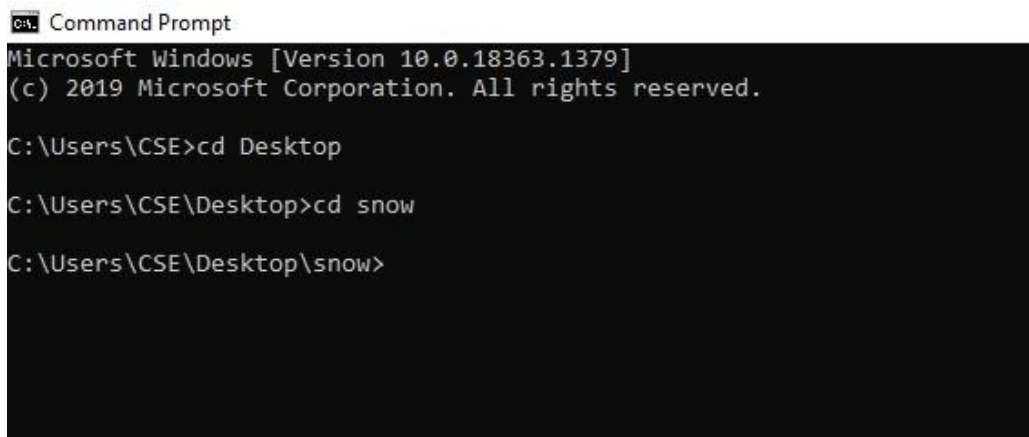


Figure: Changing the Directory

- 4) Type the Command:

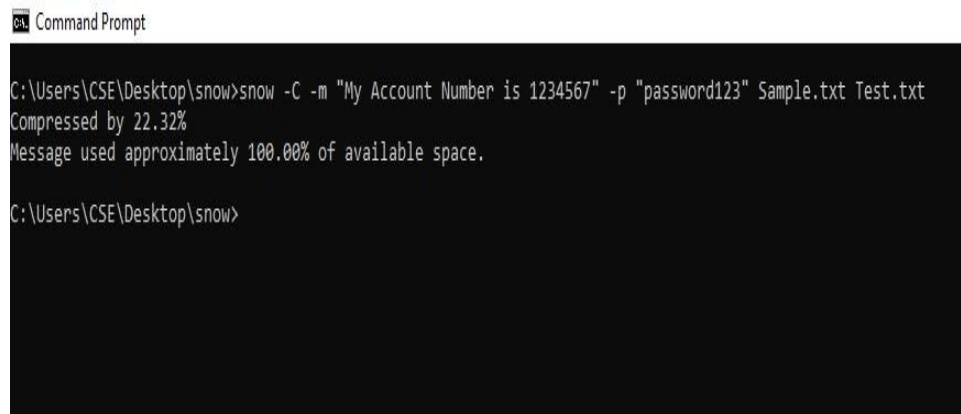
snow -C -m "text to be hidden " -p "password" <Source File><Destination File>

5) Example:

Snow -C -m "My Account number 1234567" -p
"password123" Sample.txt Test.txt

The Source file is a Sample.txt file as shown above.

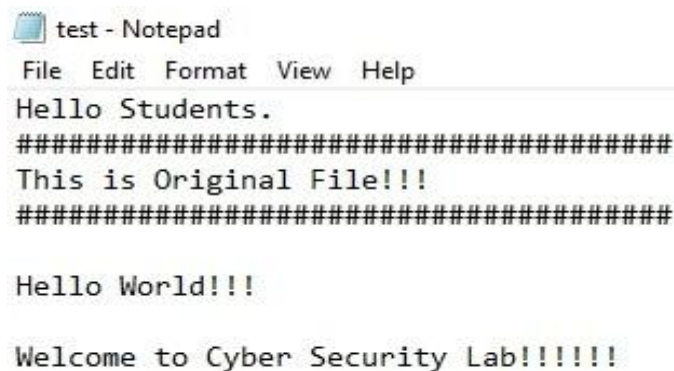
Destination file will be created automatically and exact copy of source file containing hidden information.



```
Command Prompt
C:\Users\CSE\Desktop\snow>snow -C -m "My Account Number is 1234567" -p "password123" Sample.txt Test.txt
Compressed by 22.32%
Message used approximately 100.00% of available space.
C:\Users\CSE\Desktop\snow>
```

Figure: White Space Steganography using Snow Tool

6) **Go to the Directory:** You will find a new File by name Test.txt. Open the file



```
test - Notepad
File Edit Format View Help
Hello Students.
#####
This is Original File!!!
#####

Hello World!!!

Welcome to Cyber Security Lab!!!!!!
```

Figure: File Containing Hidden Encrypted Information

7) New file has the same text as an Original file (Sample.txt) without any hidden information. This file can be sent to the target.

8) **Recovering the Hidden Information :**

On the Destination, the receiver can reveal information by using the command snow -C -p "password" <Destination

```
File>  
snow -C -p "password123" test.txt
```

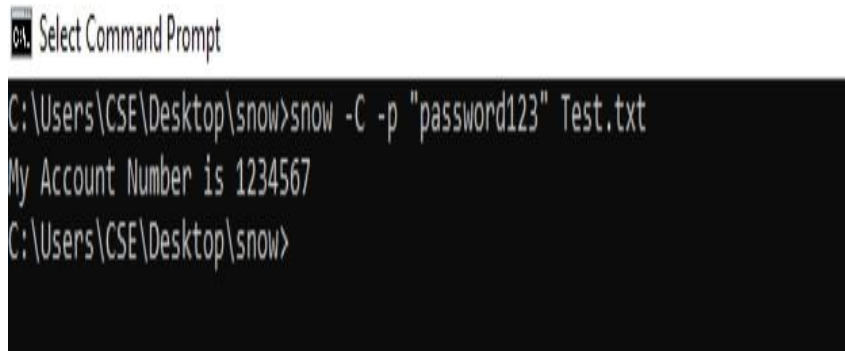


Figure: Decrypting File

As shown in the above figure, file decrypted, showing hidden information encrypted in the previous section

RESULT:

The main aim is to hide the information in the Text File Using SNOW TOOL - Text Steganography is completed successfully.

EXPT.No. 3	Write a program to illustrate Buffer overflow attack	DATE:
-------------------	---	--------------

AIM:

The main aim is to write a program to illustrate buffer overflow attack.

PROCEDURE:

A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. If the transaction overwrites executable code, it can cause the program to behave unpredictably and generate incorrect results, memory access errors, or crashes.

```
#include <stdio.h>
#include <string.h>
int main(void)
{
char buff[15];
int pass = 0;
printf("\n Enter the password : \n");
gets(buff);
if(strcmp(buff, "thegEEKstuff"))
{
printf ("\n Wrong Password \n");
}
else
{
printf ("\n Correct Password \n");
pass = 1;
}
if(pass)
{
/* Now Give root or admin rights to user*/
printf ("\n Root privileges given to the user \n");
}
```



```
}  
return 0;  
}
```

The program above simulates scenario where a program expects a password from user and if the password is correct then it grants root privileges to the user.

Let's the run the program with correct password ie 'thegeekstuff' :

OUTPUT

RUN1

Enter the password :

thegeekstuff

Correct Password

Root privileges given to the user

This works as expected. The passwords match and root privileges are given. But do you know that there is a possibility of buffer overflow in this program. The gets() function does not check the array bounds and can even write string of length greater than the size of the buffer to which the string is written. Now, can you even imagine what can an attacker do with this kind of a loophole?

Here is an example :

RUN 2

Enter the password :

hhhhhhhhhhhhhhhhhhhhhh

Wrong Password

Root privileges given to the user

RESULT:

The main aim is to write a program to illustrate buffer overflow attack is completed successfully

EXPT.No. 4	Write the steps to Download a website using Website Copier tool (HTTrack) to perform passive reconnaissance	DATE:
-------------------	---	--------------

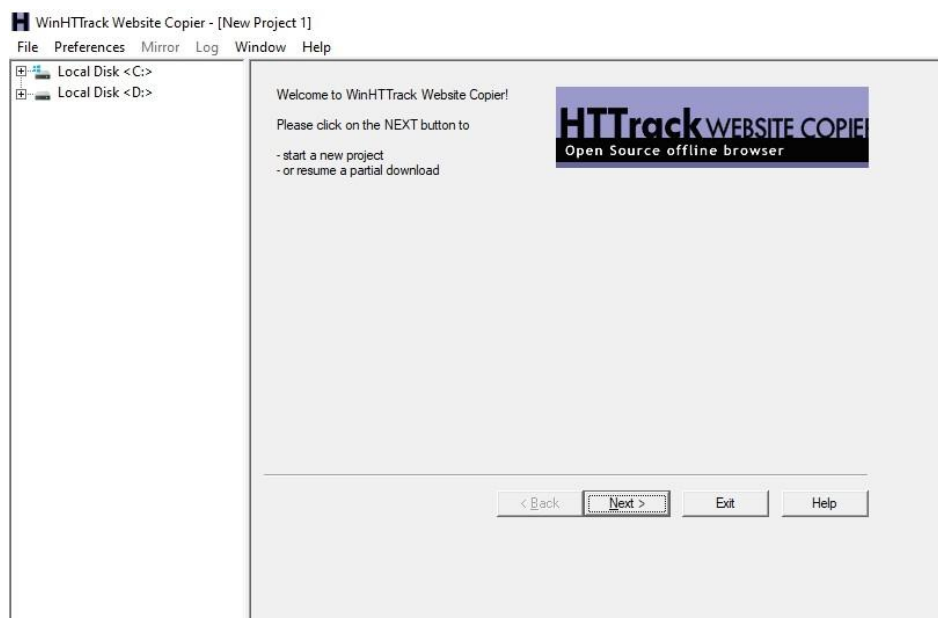
AIM:

The main aim is to downloading a website using website copier tool (HTTack)

PROCEDURE:

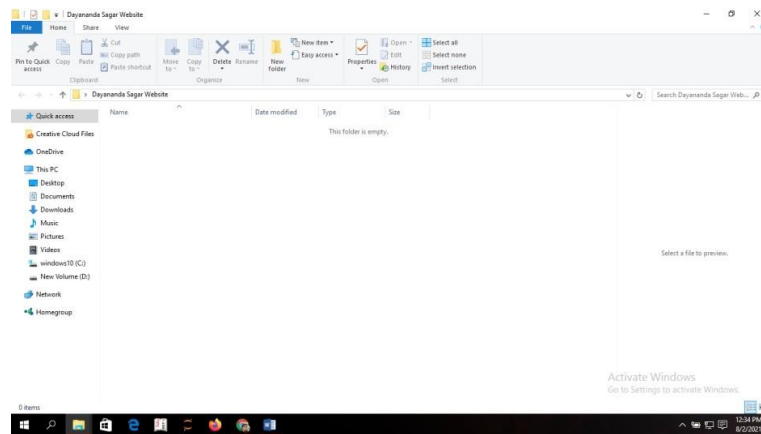
- HTTrack is a free (GPL, libre/free software) and easy-to-use offline browser utility. It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer.
- HTTrack arranges the original site's relative link-structure.
- Simply open a page of the "mirrored" website in your browser, and you can browse the site from link to link, as if you were viewing it online.
- HTTrack can also update an existing mirrored site, and resume interrupted downloads. HTTrack is fully configurable, and has an integrated help system.
- WinHTTrack is the Windows (from Windows 2000 to Windows 10 and above) release of HTTrack, and WebHTTrack the Linux/Unix/BSD release.

STEP 1: Install WinHTTrack

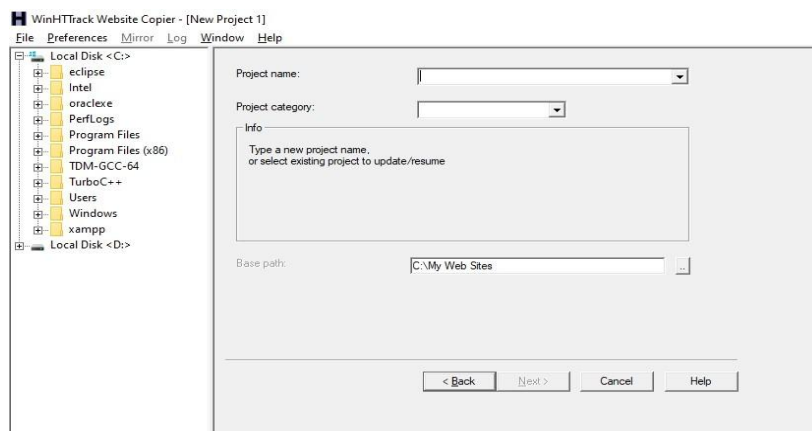


STEP 2: Create a folder on the Desktop and rename the folder For Example: Folder name is “Dayananda Sagar Website”.

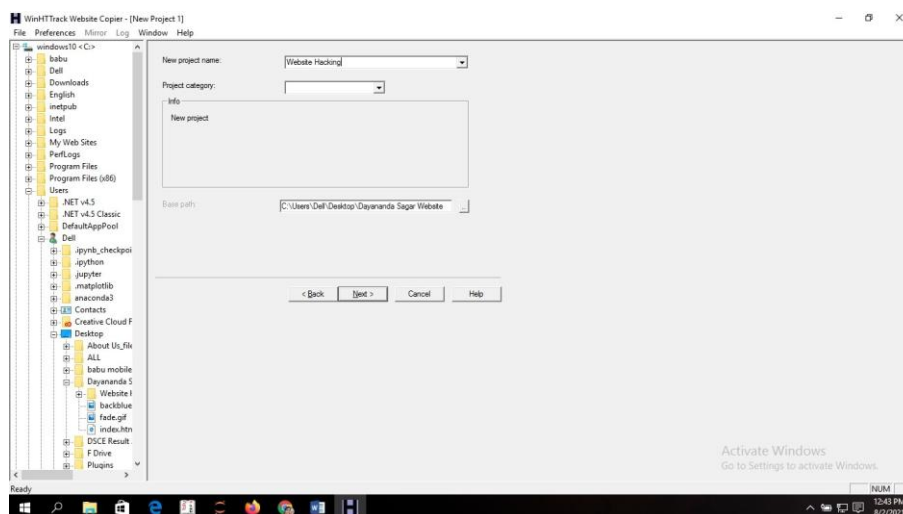
Open the folder “Dayananda Sagar Website”. The content of the folder is empty.



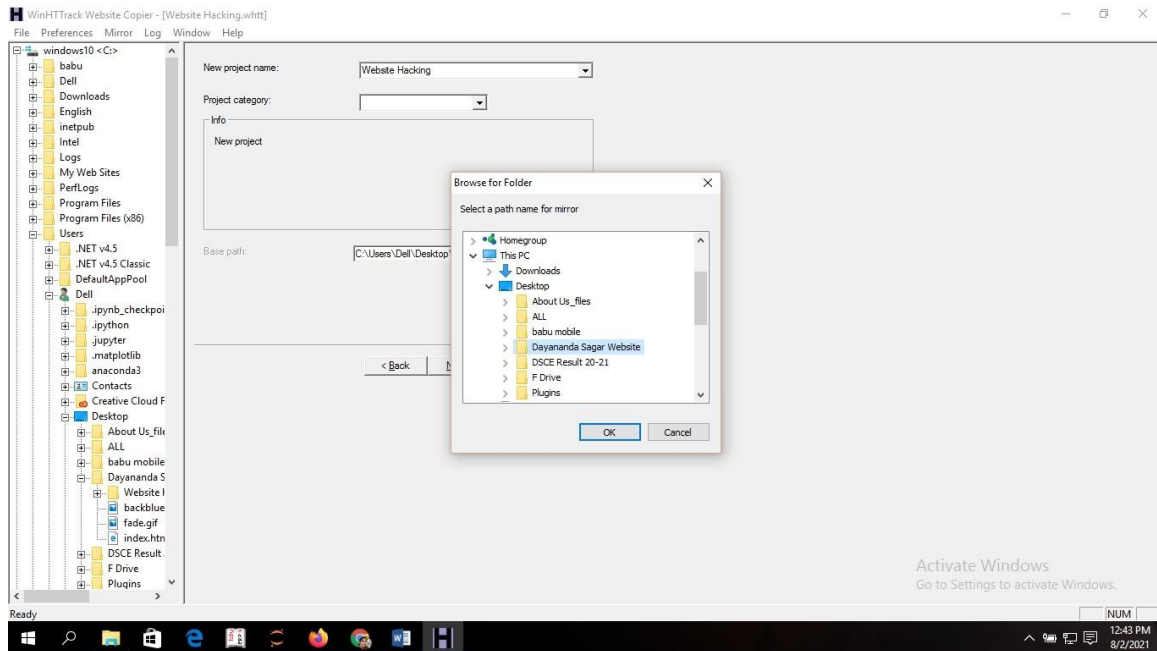
STEP 3: Select the new project from the file menu



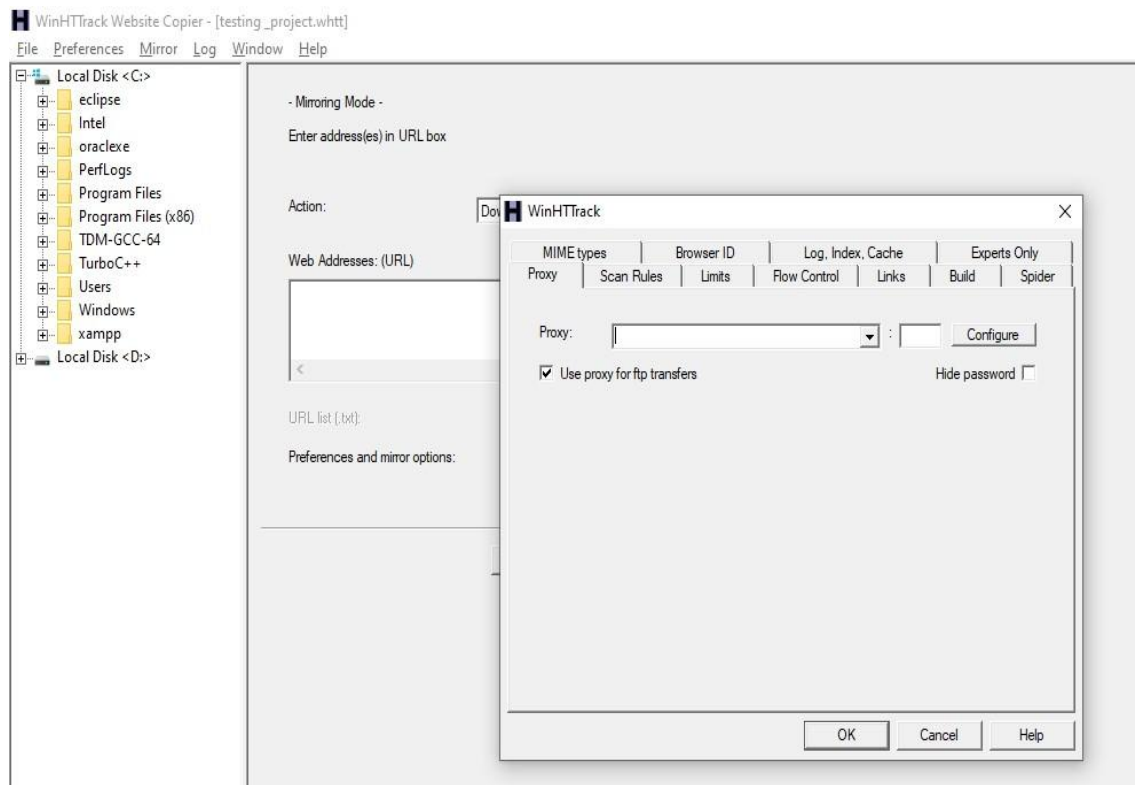
STEP 4: Enter the project name in new project field: **Example: Website hacking**



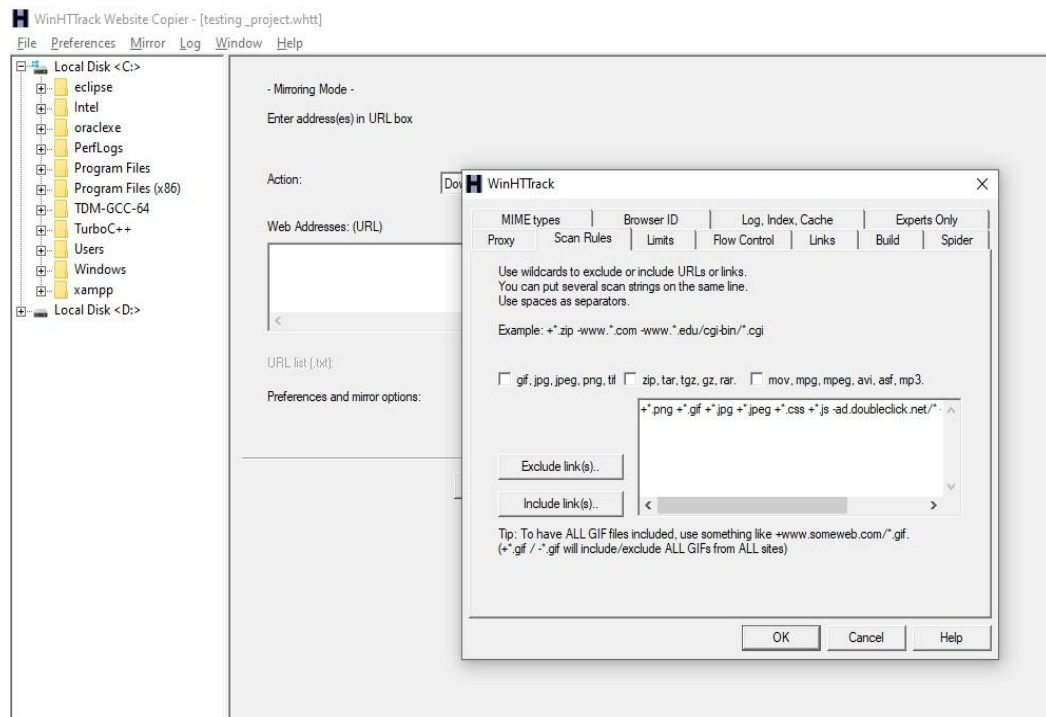
Step 5: Give the path where you need to download the files. In order to do this Click on Desktop and then click the folder “Dayananda Sagar Website”. Press OK



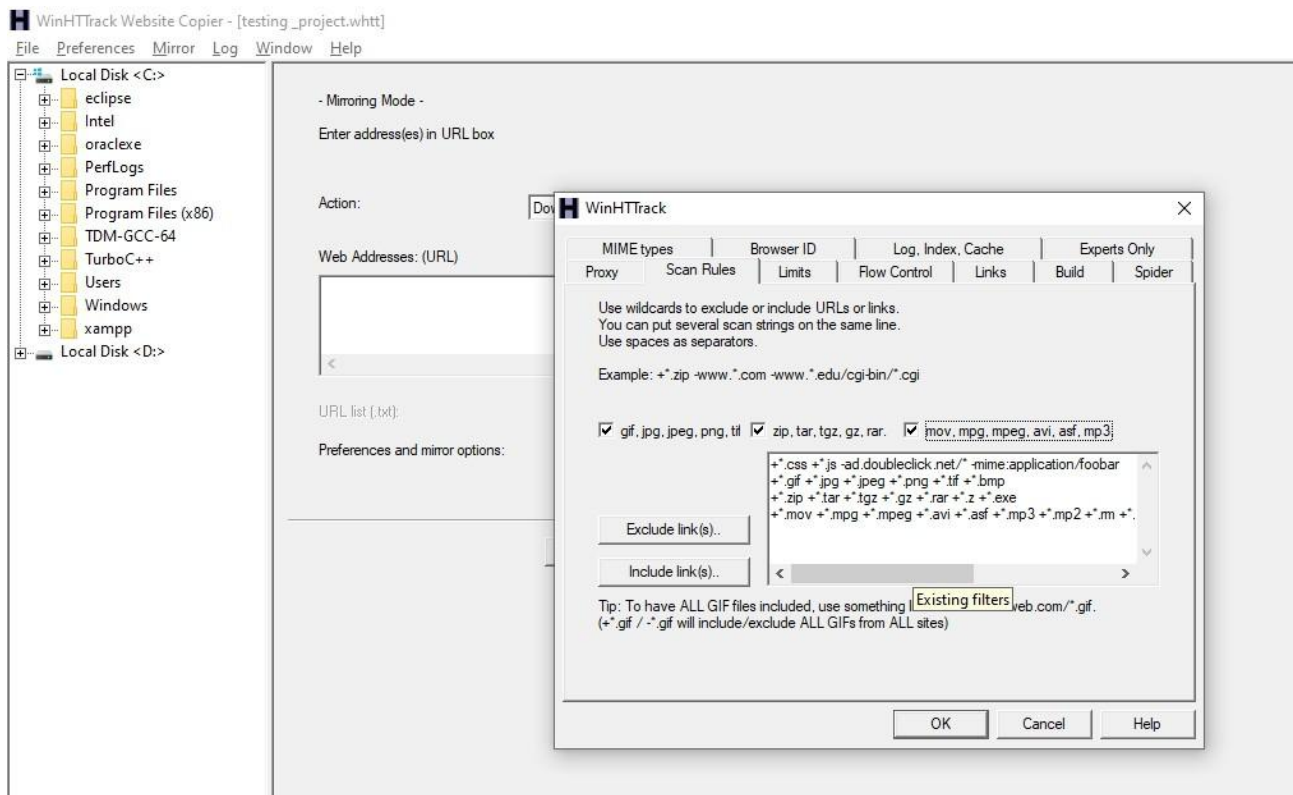
Step 6: WinHTTrack option window is opened select the scan rules



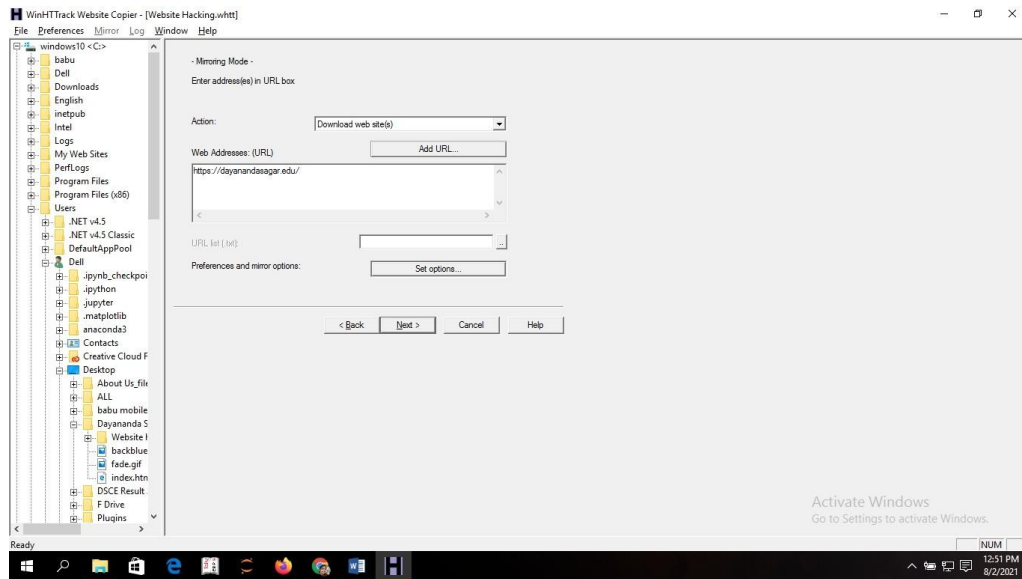
Step 7: Select all type of file to start the scan.



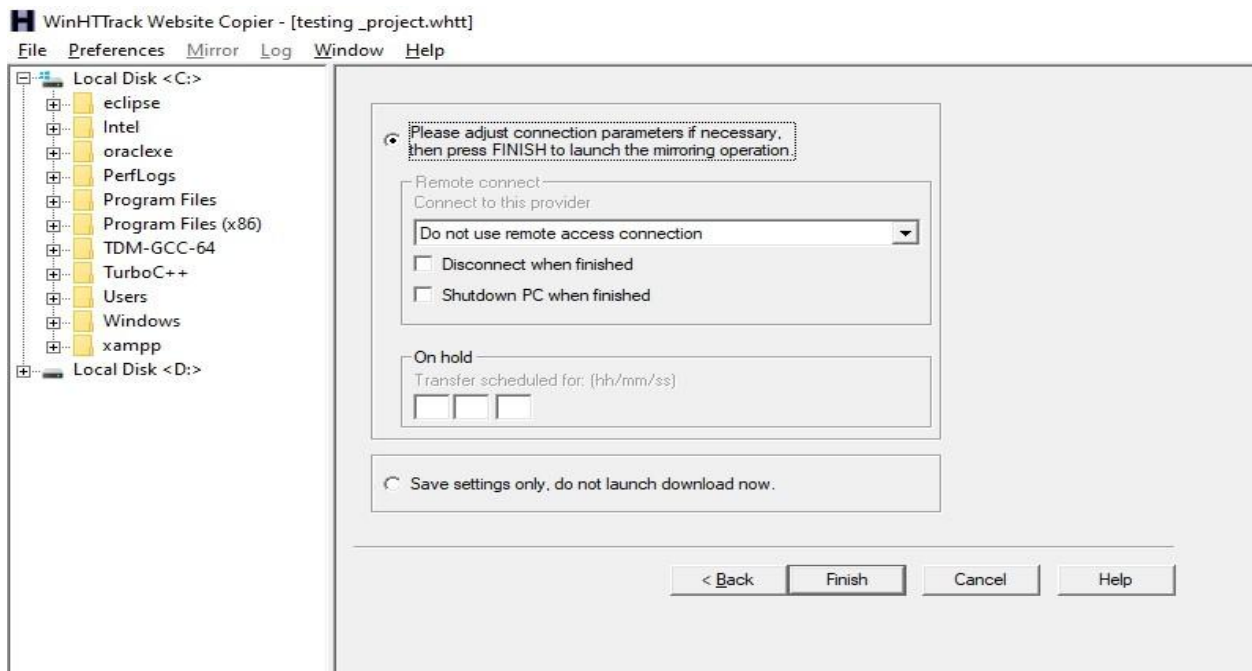
Step 8: Now all the extension is added for the scan.



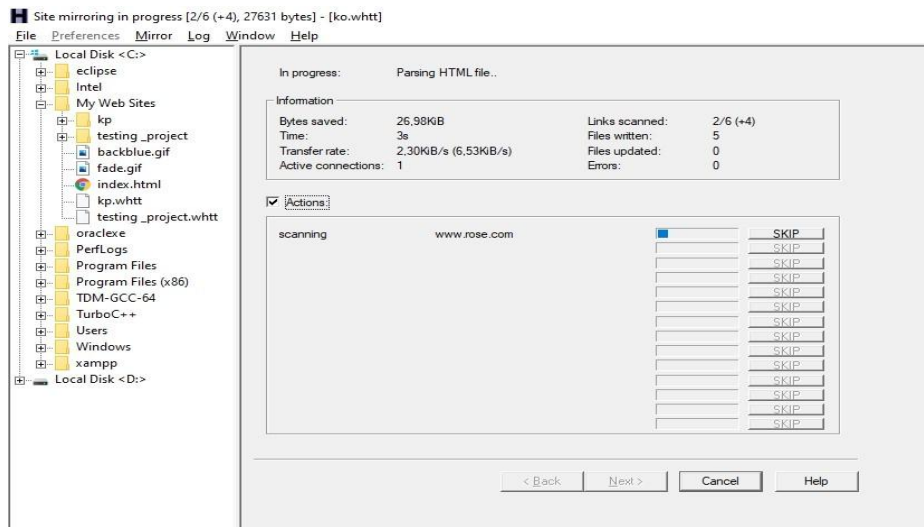
Step 9: Now type the URL address to scan



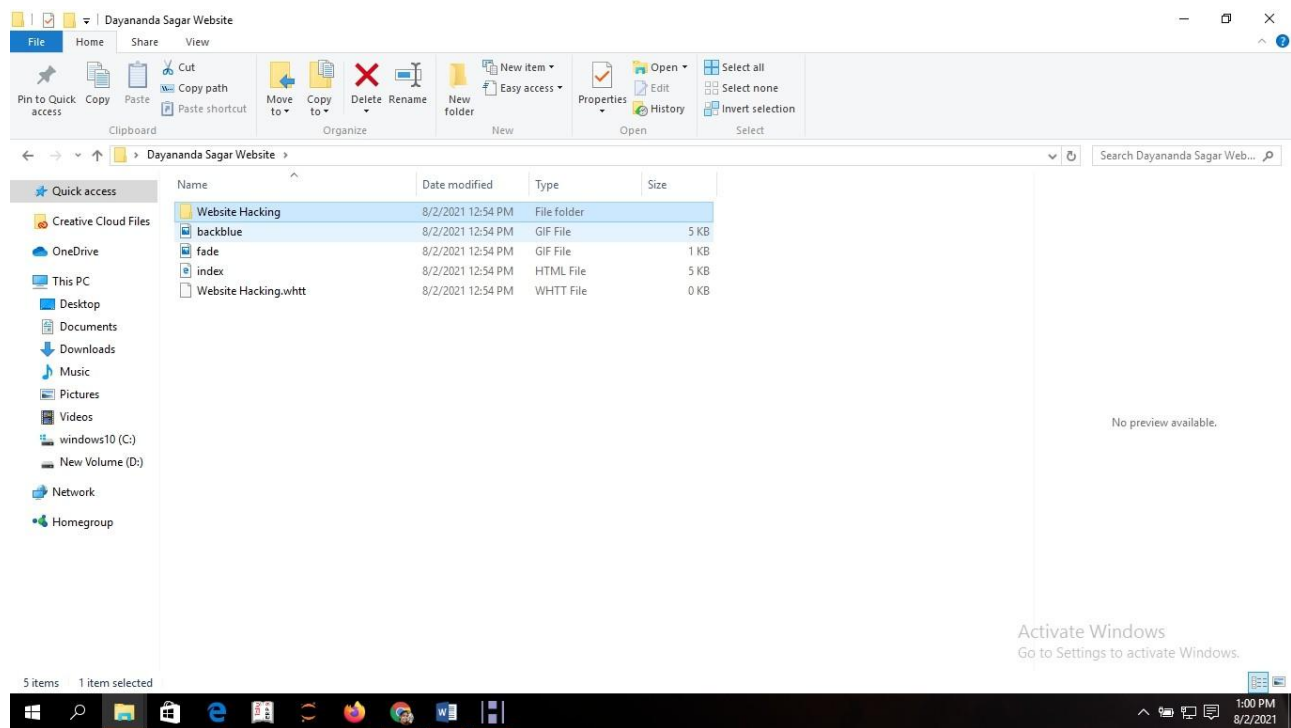
Step 10: Enable the connection adjustment if needed and click the finish button.



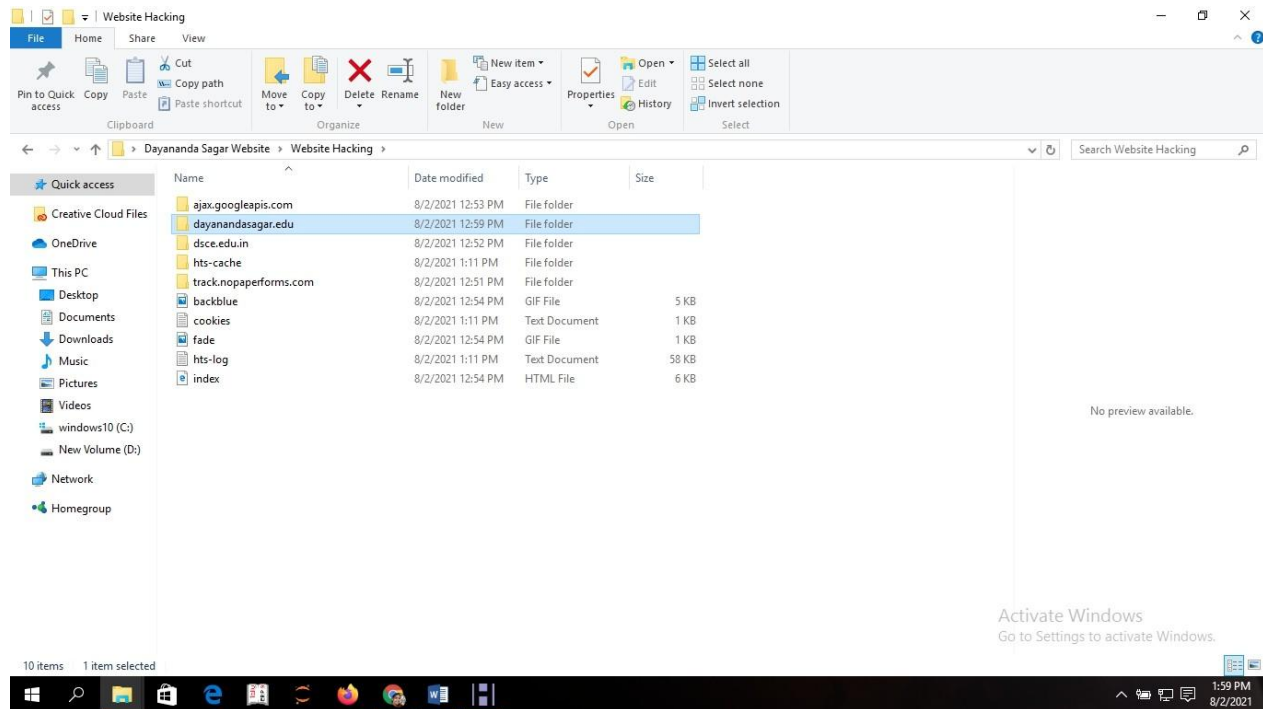
Step 11: mirroring process is get started



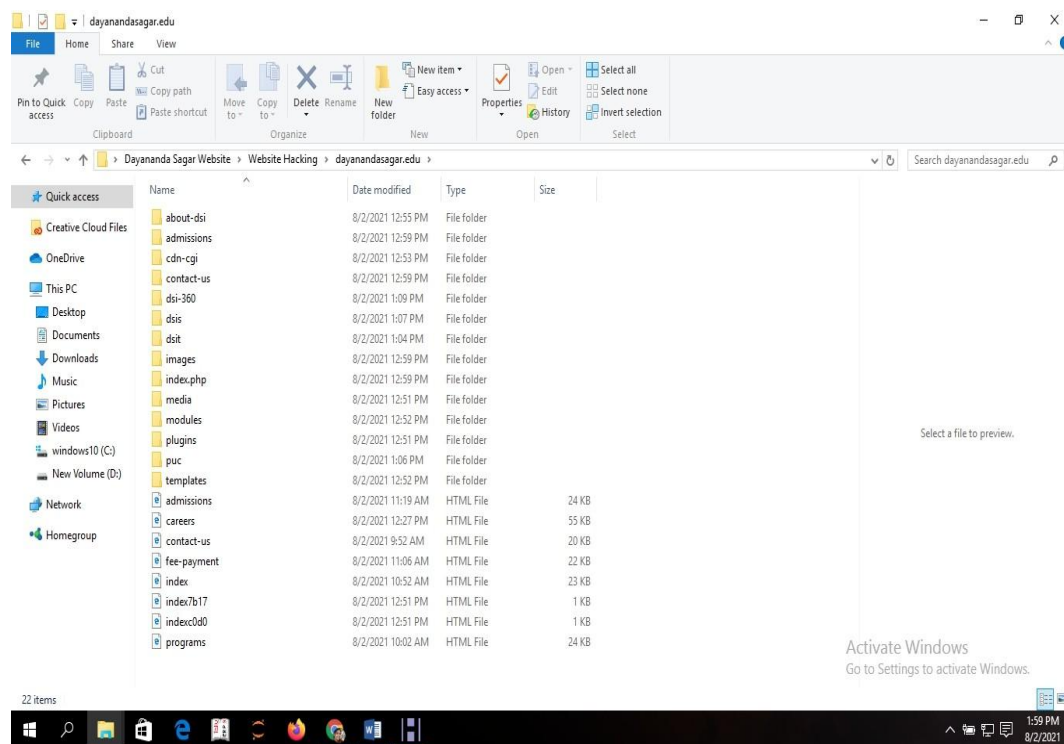
Step 12: The detail information about the URL will be fetched and saved in the folder “Dayananda Sagar Website”. You can now open the folder where you can see the project name given as Website hacking as shown in Step 3.



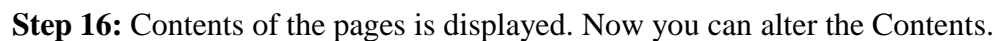
Step 13: Click on Website hacking file, then the URL address dayanandasagar.edu file given in the Step 8 will be visible.



Step 14: Click on the file, dayanandasagar.edu. Now you can find all the files of the original page of the Website.



Example: Click the file about-dsi. 3 Files are displayed. Any file can be opened in a notepad then changes can be done in the file.



The main aim is to downloading a website using website copier tool (HTTack) iscompleted successfully

EXPT.No. 5	Analyze and scan the System Vulnerabilities using Microsoft Baseline Security Analyzer (MBSA) Tool.	DATE:
-------------------	---	--------------

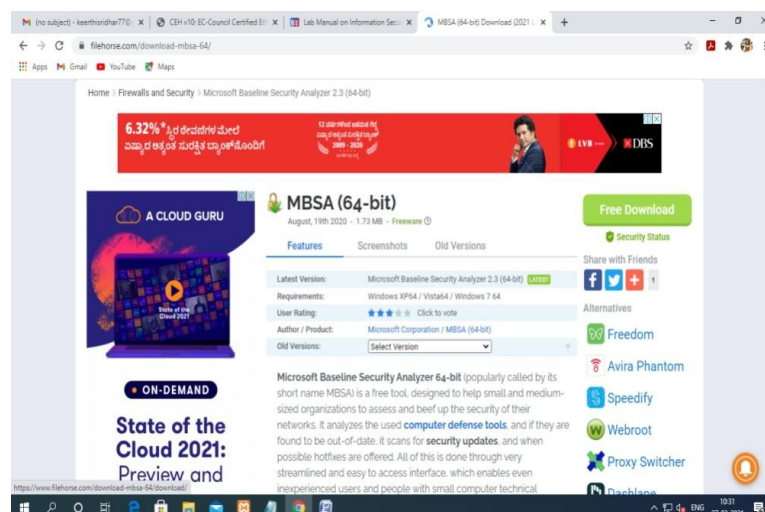
AIM:

The main aim is to scan the system vulnerabilities using Microsoft baseline security analyzer (MBSA)

PROCEDURE:

- Microsoft Baseline Security Analyzer (MBSA) is used to verify patch compliance. MBSA also performed several other security checks for Windows, IIS, and SQL Server.
- Unfortunately, the logic behind these additional checks had not been actively maintained since Windows XP and Windows Server 2003.
- Changes in the products since then rendered many of these security checks obsolete and some of their recommendations counterproductive.
- MBSA was largely used in situations where neither Microsoft Update nor a local WSUS or Configuration Manager server was available, or as a compliance tool to ensure that all security updates were deployed to a managed environment.
- While MBSA version 2.3 introduced supports for Windows Server 2012 R2 and Windows 8.1, it has since been deprecated and no longer developed. MBSA 2.3 is not updated to fully support Windows 10 and Windows Server 2016.

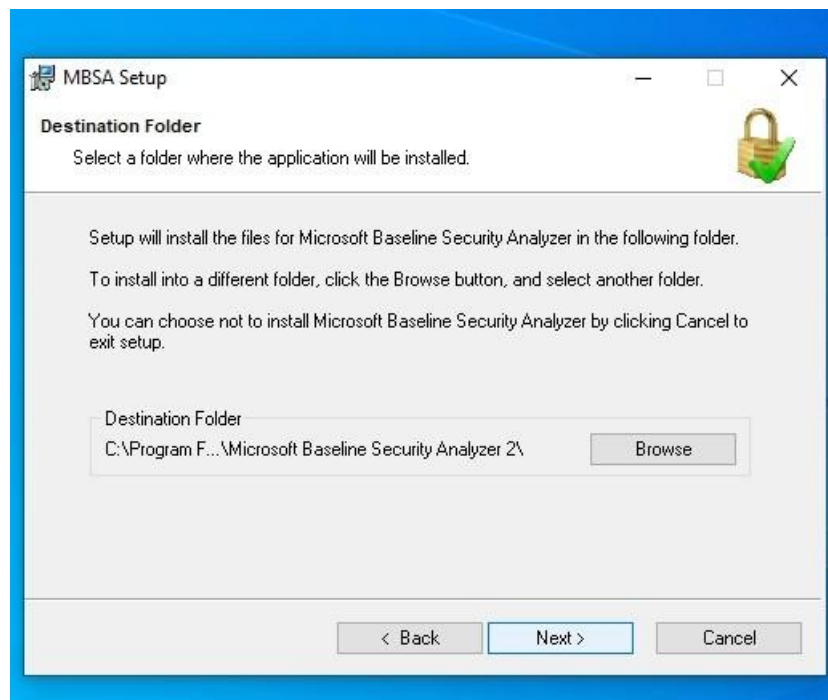
Step 1: download the Microsoft Baseline Security Analyzer (MBSA)



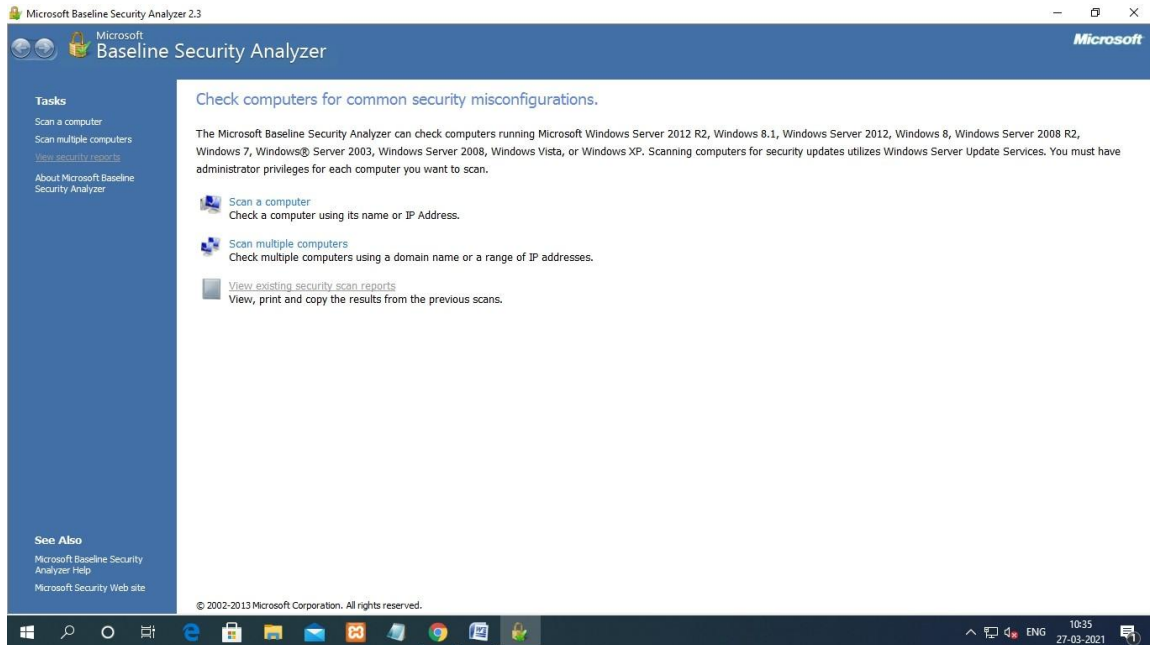
Step2: start and install the Microsoft Baseline Security Analyzer (MBSA) click next to start install



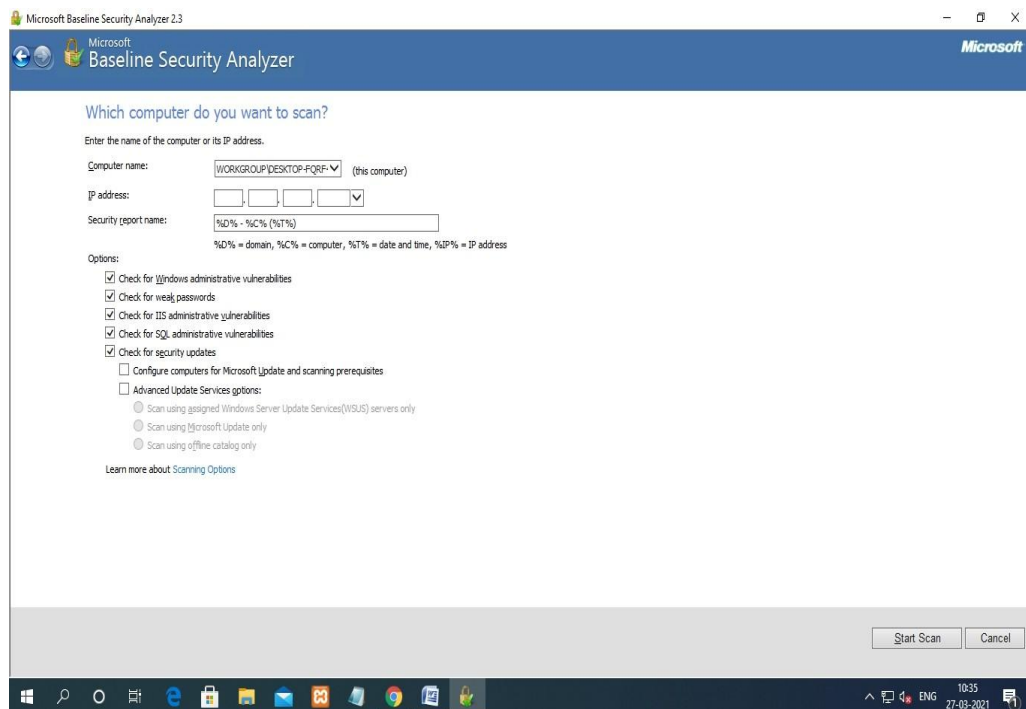
Step3: choose the location to install MBSA



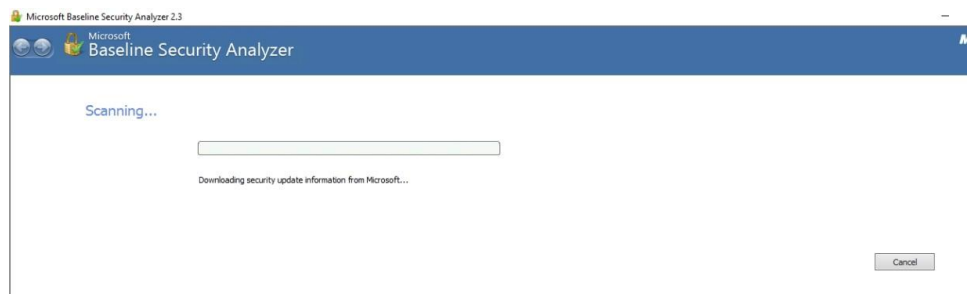
STEP 4:click the scan a computer to start the MBSA



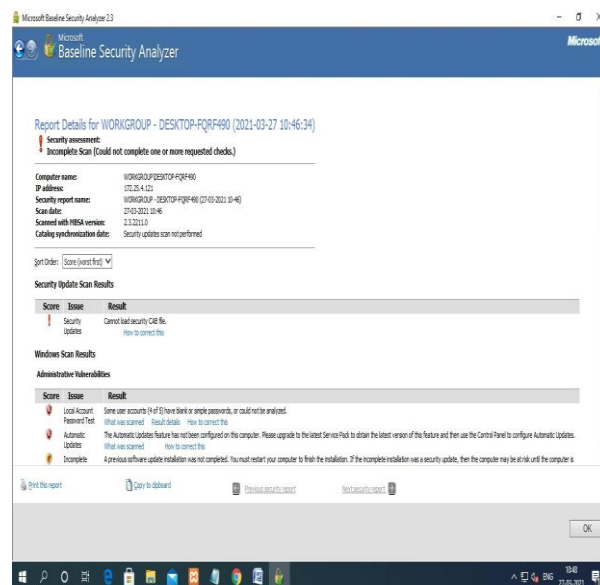
Step 5: provide the IP address and click start scan



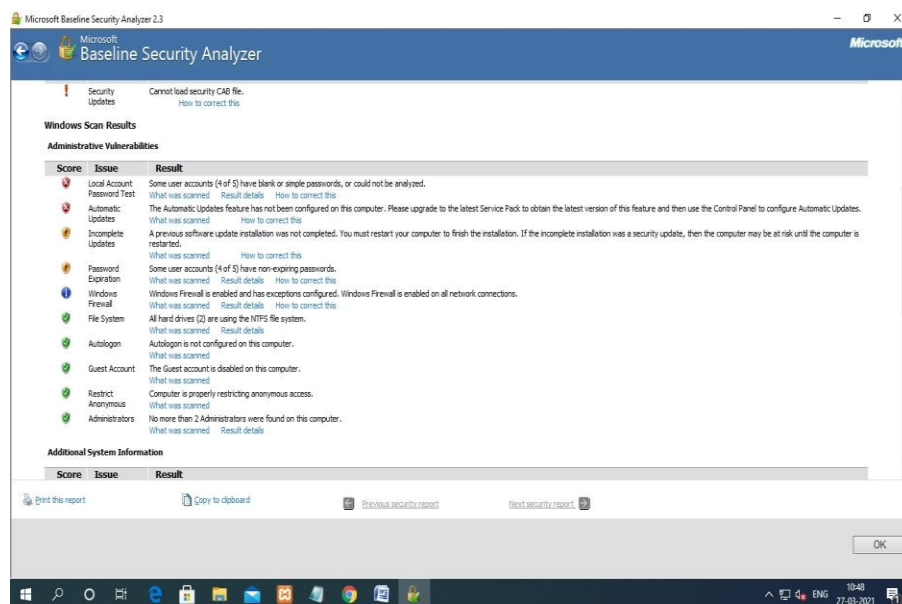
Step 7: The scanning process is GET STARTED



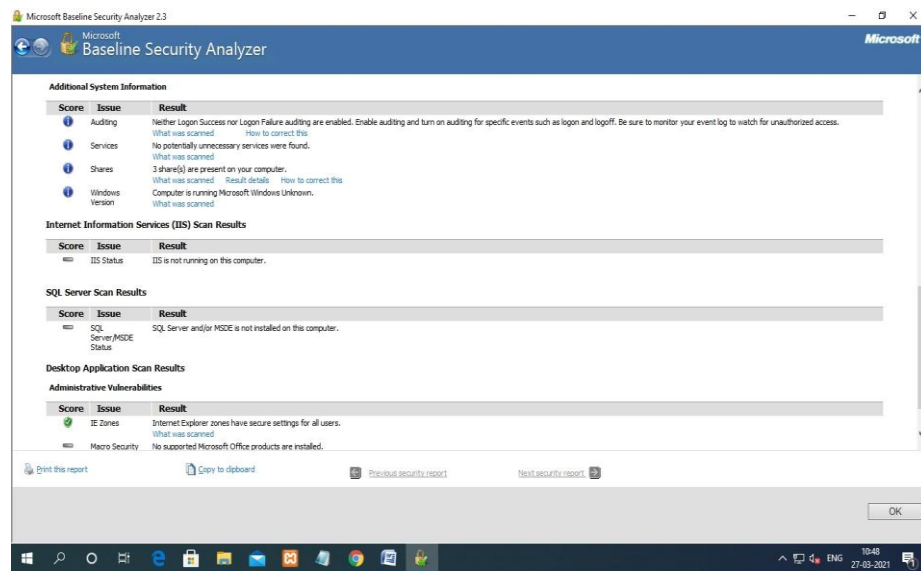
Step 8: The detail report is generated for the system



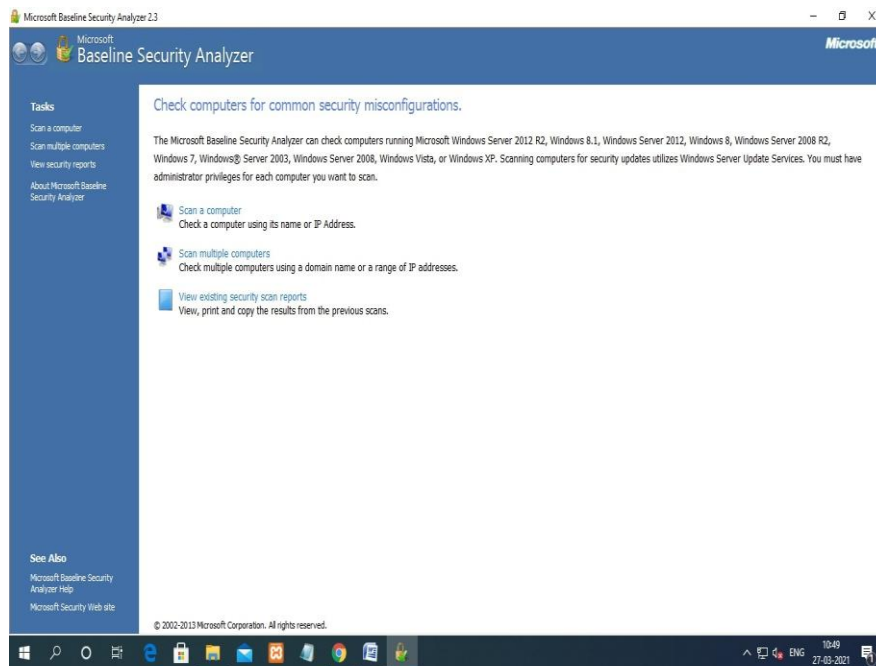
Result about the administrative vulnerabilities



Result about the additional system information, IIS scans result, desktop application



And also we can view the existing scan report



RESULT:

The main aim is to scan the system vulnerabilities using Microsoft baselinesecurity analyzer (MBSA) is completed successfully.