DAYANANDA SAGAR College OF ENGINEERING

(An Autonomous Institution affiliated to

Visvesvaraya Technological University, Belgravia)

Department of Computer Science & Engineering

SIXTH SEMESTER

CYBER SECURITY LAB MANUAL

Sub Code: 19CS6DLCSL

DAYANANDA SAGAR COLLEGE OF ENGINEERINGDEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DSCE
DEPARTMENT OF COMPUTER SCIENCE

Vision and Mission of the Department

Vision

To provide a vibrant learning environment in computer science and engineering with focus on industry needs and research, for the students to be successful global professionals contributing to the society.

Mission

*** To adopt a contemporary teaching learning process with emphasis on hands on and collaborative learning**

*** To facilitate skill development through additional training and encourage student forums for enhanced learning.**

*** To collaborate with industry partners and professional societies and make the students industry ready.**

*** To encourage innovation through multidisciplinary research and development activities**

*** To inculcate human values and ethics to groom the students to be responsible citizens.**

DAYANANDA SAGAR COLLEGE OF ENGINEERINGDEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DSCE
DEPARTMENT OF COMPUTER SCIENCE

Code of Conduct in the Lab

Do's

Students shall

- Come prepared for the program to be developed in the laboratory.
- Report any broken plugs or exposed electrical wires to your faculty/laboratory technician immediately.
- Turn off the machine once you have finished using it.
- Maintain silence while working in the lab.
- Keep the Computer lab premises clean and tidy.
- Place backpacks under the table or computer counters.
- Treat fellow users of the laboratory, and all equipment within the laboratory, with the appropriate level of care and respect.

Don'ts

Students shall not

- Talk on cell phones in the lab.
- Eat or drink in the laboratory.
- Touch, connect or disconnect any plug or cable without the faculty/laboratory technician's permission.
- Install or download any software or modify or delete any system files on any lab computers.
- Read or modify other users' files.
- Meddle with other users' files.
- Leave their personal belongings unattended. We are not responsible for any theft.

Course Objectives and Course Outcomes:

Course Objectives:

- **To be familiar with different types of Tools and methods used in Cyber Crime.**
- **To be fluent with various security measures for handling different types Cyber- attacks.**
- **To be able to analyze and implement protection and prevention of Cyber Crime Attacks.**

Course Outcomes: At the end of the course, student will be able to:

CO1	**Analyze and apply the security features on web browsers**
CO2	**Investigate the system vulnerabilities to protect system from Cyberattack**
CO3	**Apply different cyber security tools**
CO4	**Analyze the apply Forensic tool for cyber crime investigation**
CO5	**Analyze and Evaluate real time Network Traffic by capturing the network packets**

ExpT.No		Contents of the Experiment	Hours	Cos
1)	a)	**Write the Steps to ensure Security of any one web browser (Mozilla Firefox/Google Chrome).**	**01**	**CO1**
	b)	**Write the commands for Gathering Information about the active websites using Windows Command line Utilities.**	**01**	**CO1**
2)	a)	**Validate the Password Cracking technique on an authorized MS Excel Document.**	**01**	**CO3**
	b)	**Scanning System Vulnerabilities using Microsoft Baseline Security Analyzer (MBSA) Tool.**	**01**	**CO2**
3)	a)	**Study of Cyber Forensic Tools.**	**01**	**CO4**
	b)	**Comparison of two files for Forensic Investigation by Compare It Tool**	**01**	**CO4**
4)	a)	**Analyse the Port vulnerability of the system using NMAP to ensure security in Apache Server**	**01**	**CO2**
	b)	**Steganography - Hiding and Recovering The Information Using QUICKSTEGO TOOL**	**01**	**CO3**
5)	a)	**Write a program to illustrate Buffer overflow attack..**	**01**	**CO3**
	b)	**Implement a versatile hacking tool - Hashcat Tool for cracking the password.**	**01**	**CO3**
6)	a)	**Implement website Defacing Attack using Website Copier tool (HTTrack)**	**01**	**CO3**
	b)	**Text Stegnography : Hiding The Information In The Text File Using Snow Tool**	**01**	**CO3**
7)	a)	**Analyse the real time network traffic by capturing TCP packets using Wireshark tool.**	**01**	**CO5**
	b)	**Analyze the real time network traffic by capturing FTP packets using Wireshark Tool.**	**01**	**CO5**
8)	a)	**Write a C program to encrypt the secret text message by implementing Caesar Cipher substitution technique.**	**01**	**CO3**
	b)	**Investigate the Hidden Text and extract the secret information behind an image using Command Prompt.**	**01**	**CO4**

EXPT.NO 1(A)	STEPS TO ENSURE SECURITY OF ANY ONE WEB BROWSER (MOZILLA FIREFOX/GOOGLE CHROME)	DATE:

AIM:

The main aim is to study the steps to ensure security of any one web browser (Mozilla Firefox/Google chrome).

PROCEDURE:

1. Configure privacy and security settings

The point here is to disable features that can cause vulnerabilities introduced through third-party cookies as well as plug-ins, add-ons and extensions. The fewer of these features you enable, the less likely they are to be exploited by hackers.

2. Choose your warnings

Disabling features helps secure computers but also potentially prevents users from getting at resources they might need. For instance, cookies help load pages faster at often-visited websites but they can also direct users into compromised sites. To prevent that, set up cookie warnings so users are alerted before navigating to unknown sites. Don't save passwords

Allowing browsers to save passwords may be convenient but creates security risks. Malware that captures keystrokes can steal the information. Also, if a laptop falls into the wrong hands, it doesn't take much for a savvy hacker to find the stored password information.

4. Select plug-ins carefully

Java, Flash, JavaScript, ActiveX and myriad other plug-ins have all been exploited by hackers to break into computers and networks. Use these only if you have a reason to; otherwise, disable them.

5. Update browsers regularly

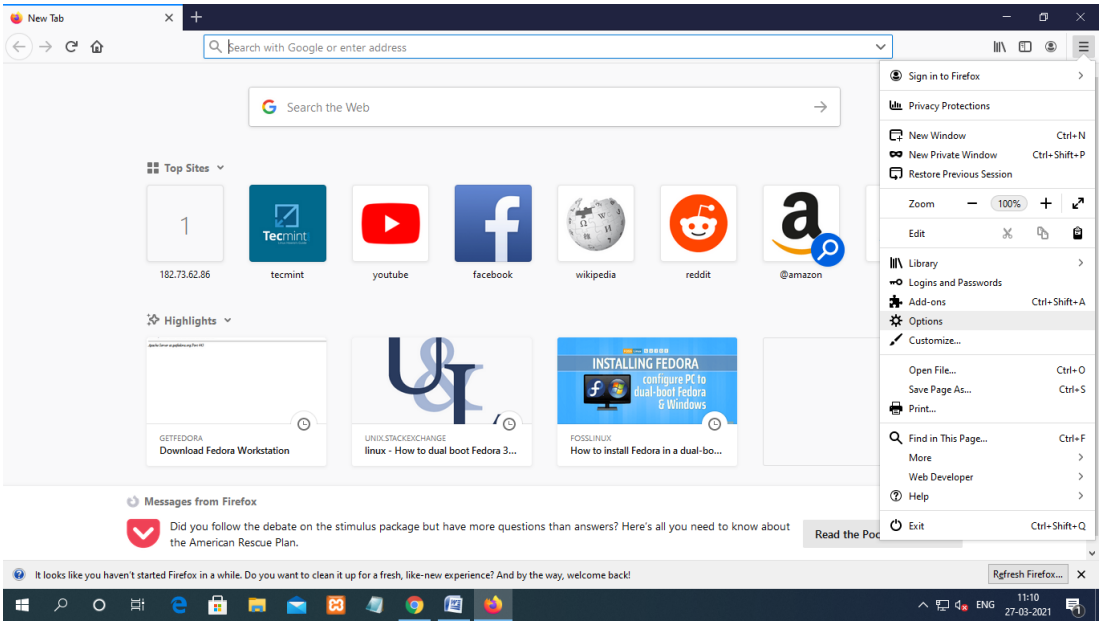
Browsers, just like any other software, need to be updated regularly to plug security holes. Out-of-date software is a favorite way for hackers to break into networks. Updates not only address security but also make browsers run better.

6. Install and update endpoint security

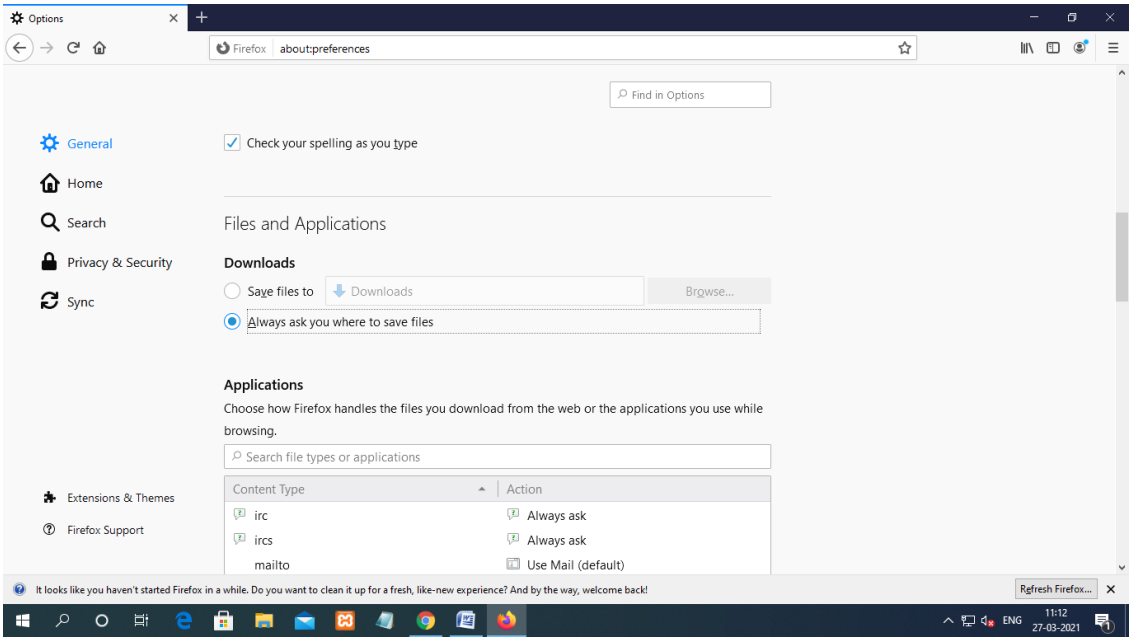
Robust endpoint security is an absolute necessity. Threats that can elude browser privacy settings can still be blocked by an endpoint security solution that helps prevent ransomware and other types of malware, and detects zero-day threats.

Firefox hacks and tips for better security

- **If you use Mozilla Firefox and want to improve your browser security settings, press the hamburger menu in the top right corner and go to "Options".**

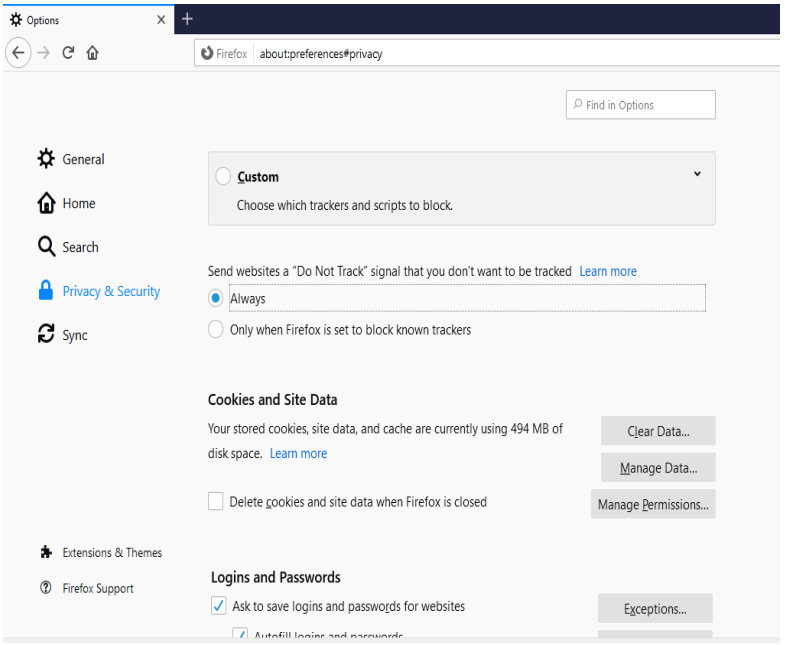


In the "General" tab, at the Downloads section, press "Always asks me where to save files". This way, you won't have a web location try to automatically save dangerous content to your computer.



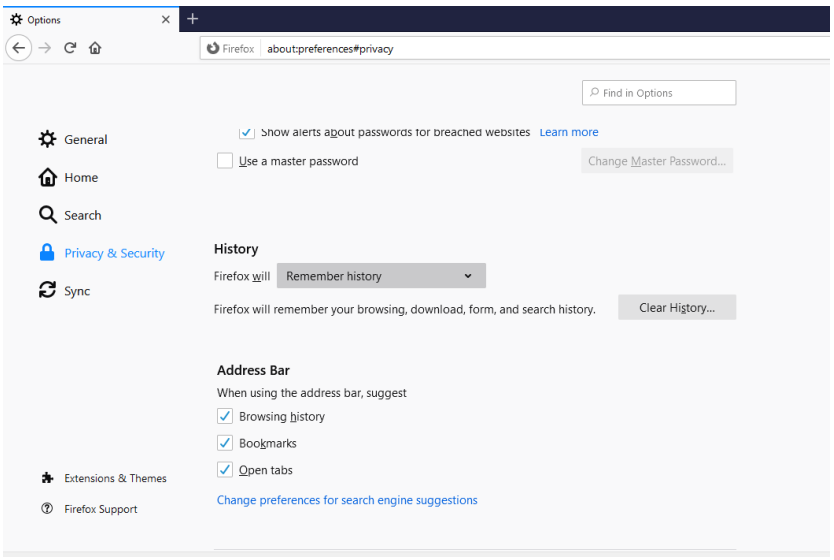
At the same time, this gives you the option to place suspicious content in a safe location where you can analyze it afterwards.

Next, go to the Privacy tab.



At the "Tracking" section press the blue text with "manage your Do Not Track settings" and check "Always apply do not track".

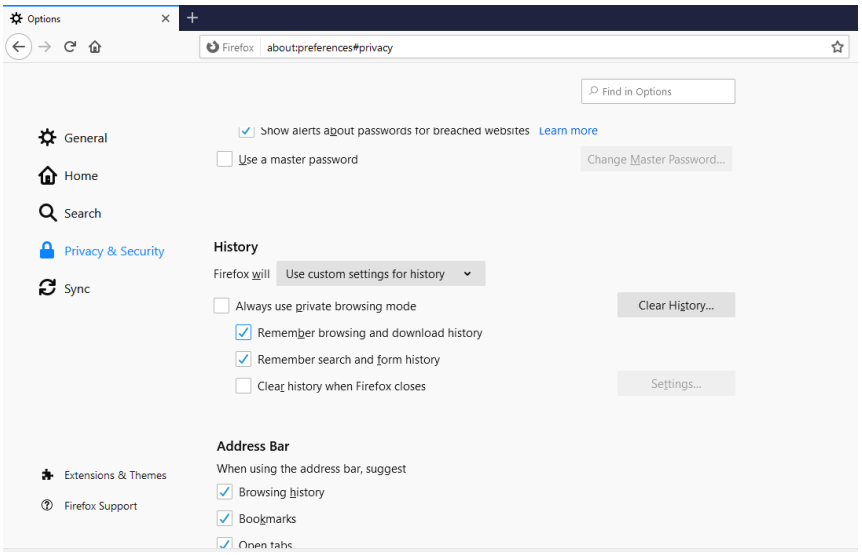
After you do this advertising, commerce and various other sites shouldn't be able to track you across the web. While in the Privacy tab, at the "History" section, choose



"Firefox will never remember history".

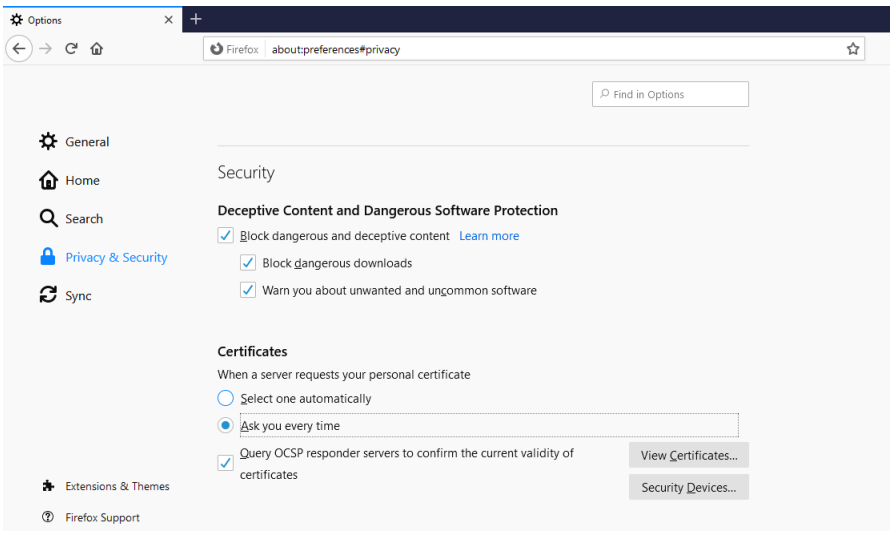
This is especially important if you know your device may be used by other people.

For a more detailed control of your history section, select "Use custom settings for history". Check "Always use private browsing mode" so every time you close your Firefox browser it will clear browsing history, search results, cookies and download history. The last changes you should make in Firefox can be found in the "Security" category.



First, make sure all of the four check boxes in the General section are checked in.

This ensures that your browser will inform you whenever websites try to install malicious add-ons and other content. In the "Logins" section you can set up a Master Password.



Doing this is especially useful when multiple people have access to the computer, since it asks you introduce a master password before you can access logins. This way, other people won't be able to access your important accounts such as email. Once more, we cannot recommend this enough, but don't let your

RESULT:

The detail studies of the steps to ensure security of any one web browser (mozilla firefox/google chrome) is completed successfully

EXPT.NO 1(B)	GATHERING INFORMATION USING WINDOWS COMMAND LINE UTILITIES	DATE:

AIM:

The main aim is to gather the information using windows command line utilities.

PROCEDURE:

Consider a network where you have access to a windows PC connected to the Internet.

Using Windows –based tools, lets gather some information about the target. You can ask any target domain or IP address, in our case, we are using example.com as a target.

Topology Diagram:

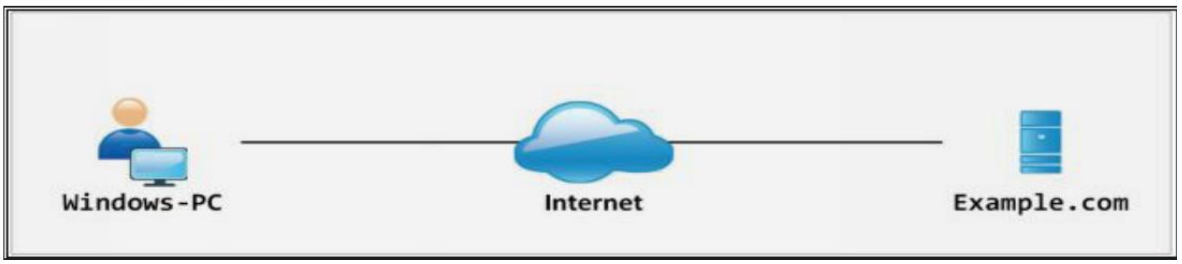
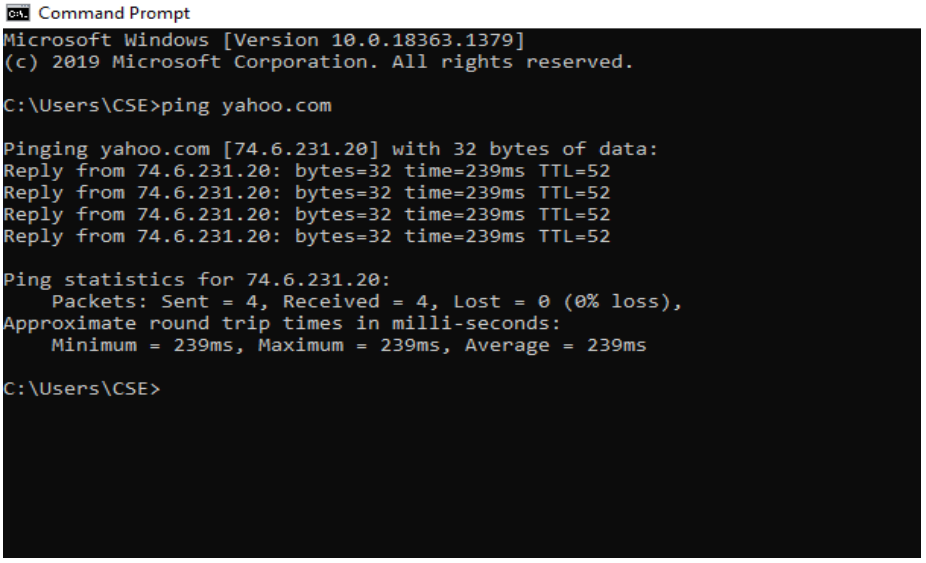


Figure: Topology Diagram

1) **Open Windows Command Line (cmd) from Windows PC.**
2) **Enter the Command "ping yahoo.com" to ping.**

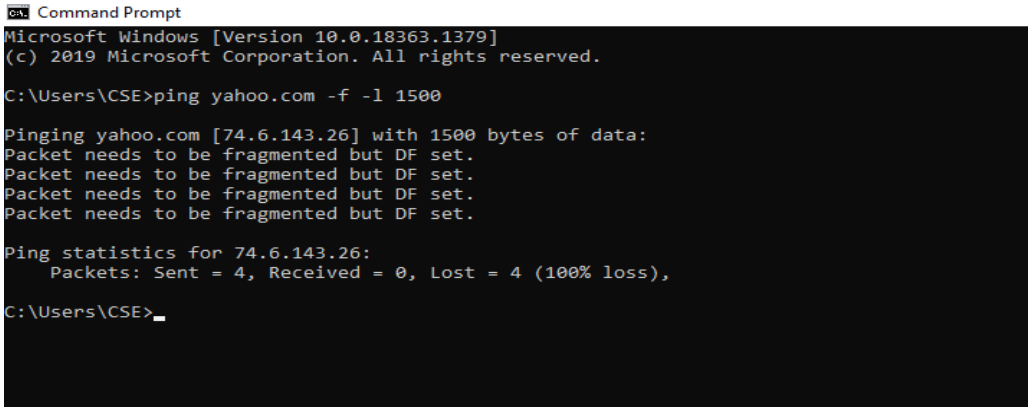


3) **From the Output you can Observe and extract the following Information:**

- **yahoo.com is live**

- **IP address of yahoo.com**
- **Round trip time**
- **TTL Value**
- **Packet Loss Statistics**

4) Now, enter the command "ping yahoo.com –f -l 1500" to check the value of fragmentation.



• Ping: a command to determine the connectivity between your computer and a particular address (within the Local network or the internet).

• URL or local address: the web address or the IP address of the server you're trying to check for speed connectivity.

• -f : a command to make sure that when you ping a certain address, it will not fragment the packet sent or received.

• -l : a command commonly known as a packet size switch. This is the best command to help you determine the best MTU size for your network.

Here are the results that you may get after doing the ping test:

• Four replies received: **This means that the packet size entered is either within or the actual MTU size used within your network.**

• Destination net unreachable: **This means that there was no path or route to the destination or the address.**

• Request Timed Out: **This means that within the default wait time period (1 second), there was no response.**

• Packet needs to be fragmented but DF set: **This means that the packet size you entered is too high for your MTU value.**

RESULT:

The detail studies of the steps to gather information about the target is completed successfully

EXPT.NO 2(a)	PASSWORD CRACKING ON AN AUTHORIZED MS EXCEL DOCUMENT	DATE:

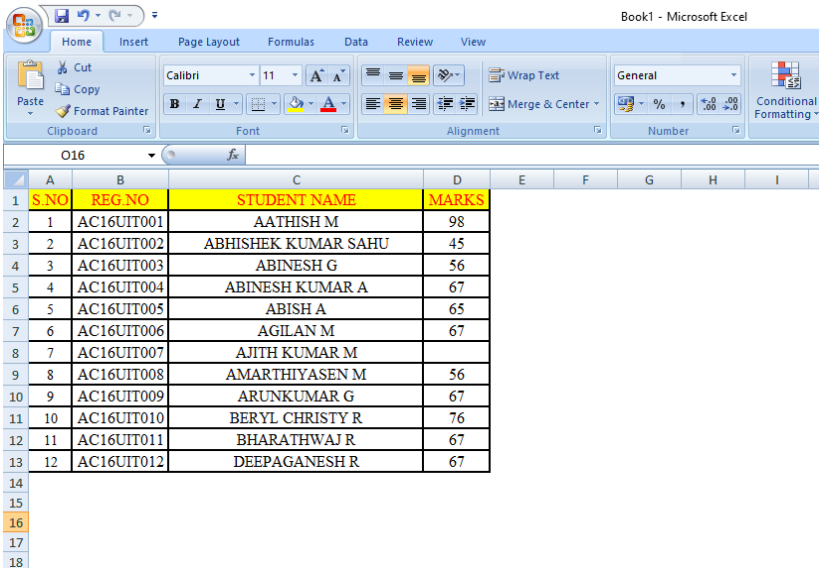
AIM:

The main aim is to open an authorized ms excel document by password cracking.

PROCEDURE:

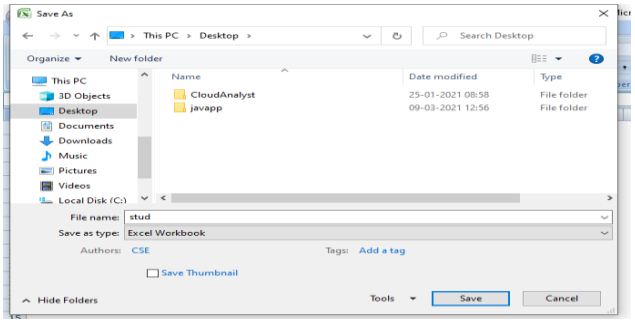
Step 1: Open the MS EXCEL by clicking start menu icon in the task bar.

Step 2: Create an any highly official document (example: student mark sheet, EMP salary, ECT….)

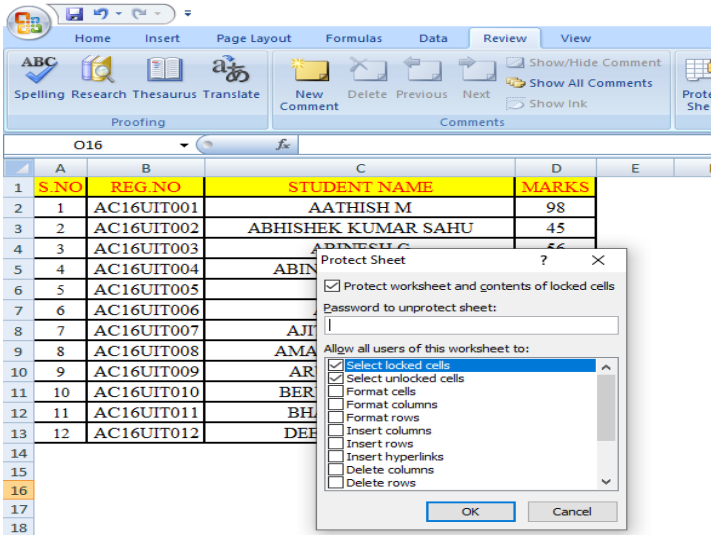


S.NO	REG.NO	STUDENT NAME	MARKS
1	AC16UIT001	AATHISH M	98
2	AC16UIT002	ABHISHEK KUMAR SAHU	45
3	AC16UIT003	ABINESH G	56
4	AC16UIT004	ABINESH KUMAR A	67
5	AC16UIT005	ABISH A	65
6	AC16UIT006	AGILAN M	67
7	AC16UIT007	AJITH KUMAR M	
8	AC16UIT008	AMARTHIYASEN M	56
9	AC16UIT009	ARUNKUMAR G	67
10	AC16UIT010	BERYL CHRISTY R	76
11	AC16UIT011	BHARATHWAJ R	67
12	AC16UIT012	DEEPAGANESH R	67

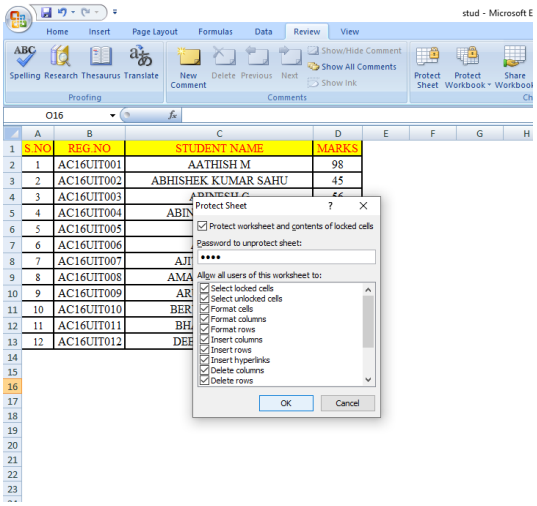
Step 3: Save the MS EXCEL document with a file name and with the extension of .xsls



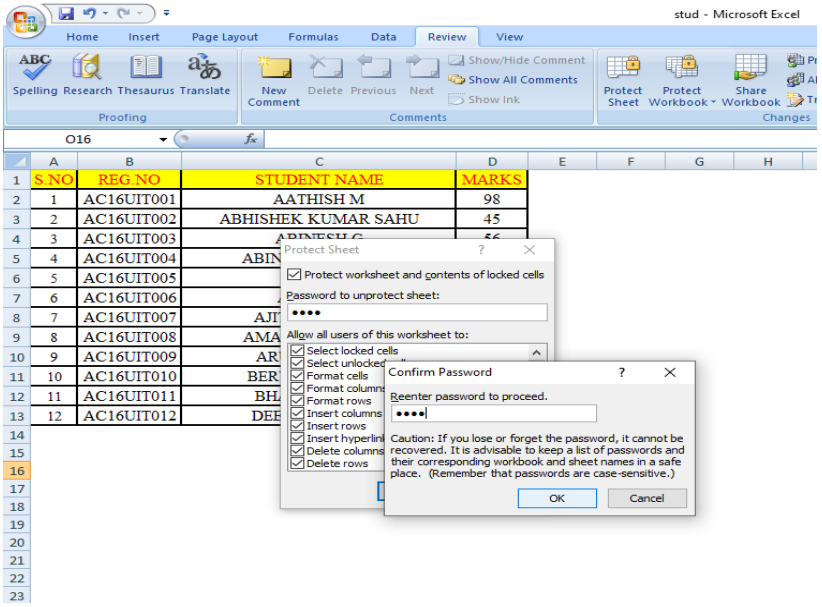
Step 4: Protect your document with a password by selecting review tab and choose protect sheet. Assign a password



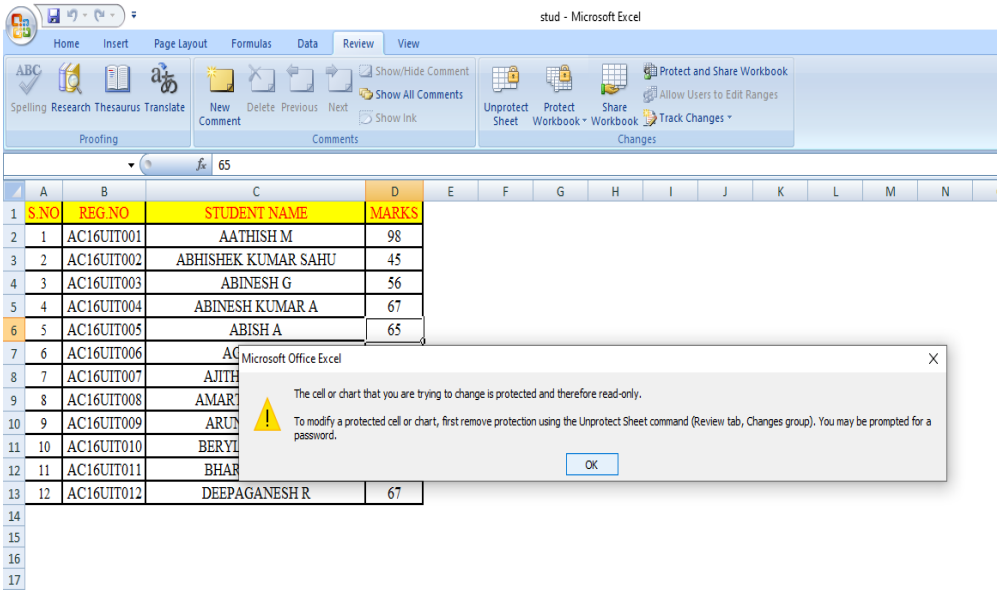
Step 5: Enable all the alignment edition option so therefore one can edit out official document. Select ok



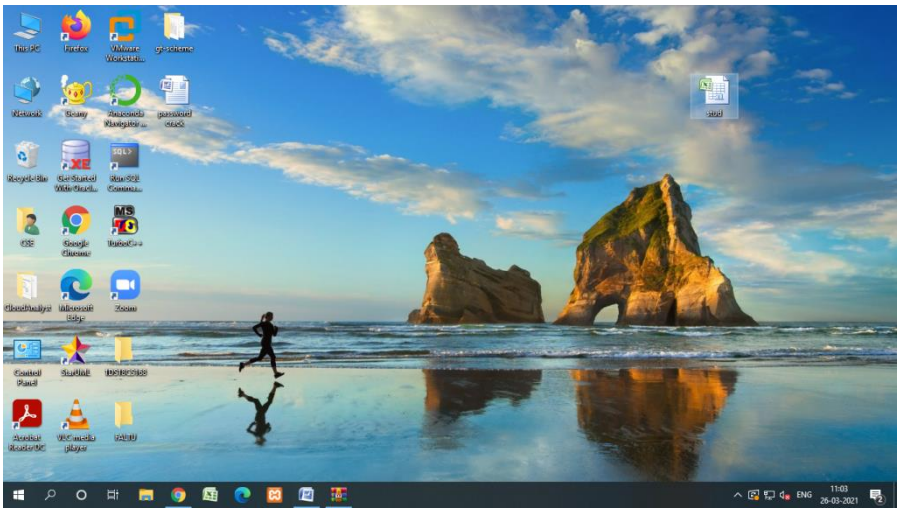
STEP 6: An d re-enter the password to conform the password



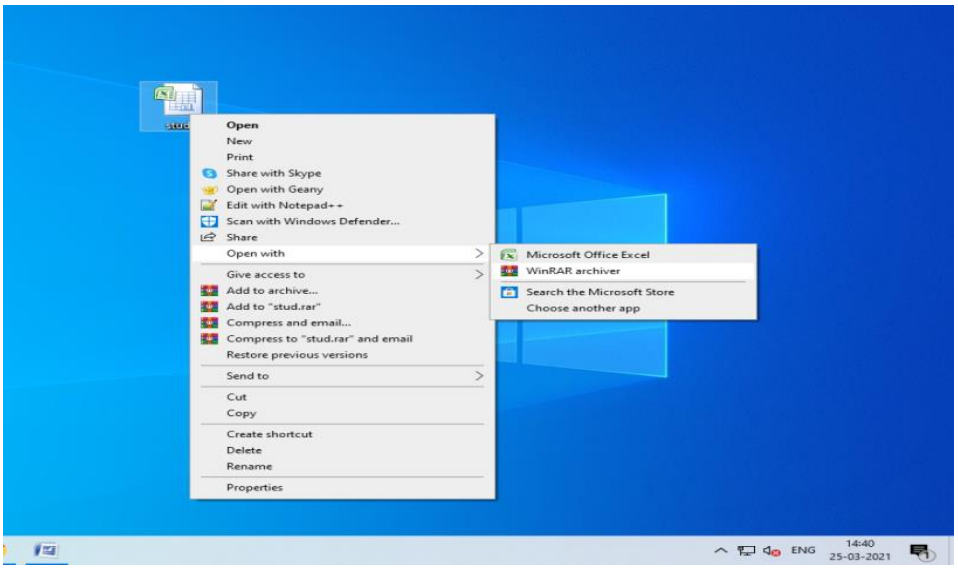
Step 7: Now check if the editing is possible in our official document. If we try to change any this will display that this document is protected by password



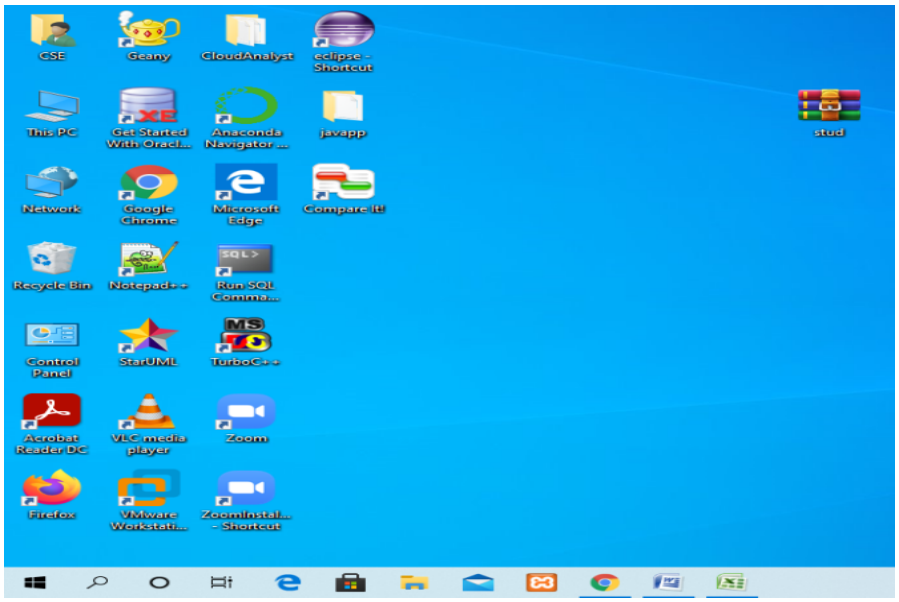
Step 8: Save the document in a new folder or in a desktop



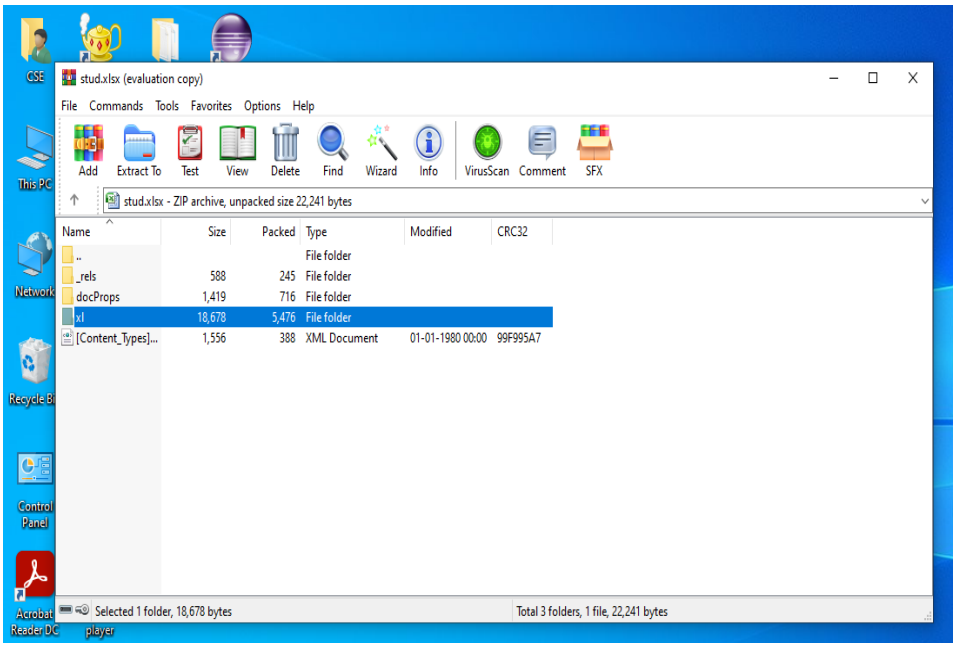
Step 9: Select the file and change the extension as .zip or right click on the file select the properties form the pop-up menu and change the extension of the document otherwise right click on the file select open with and choose winRAR. The .xsls file is changed to .zip



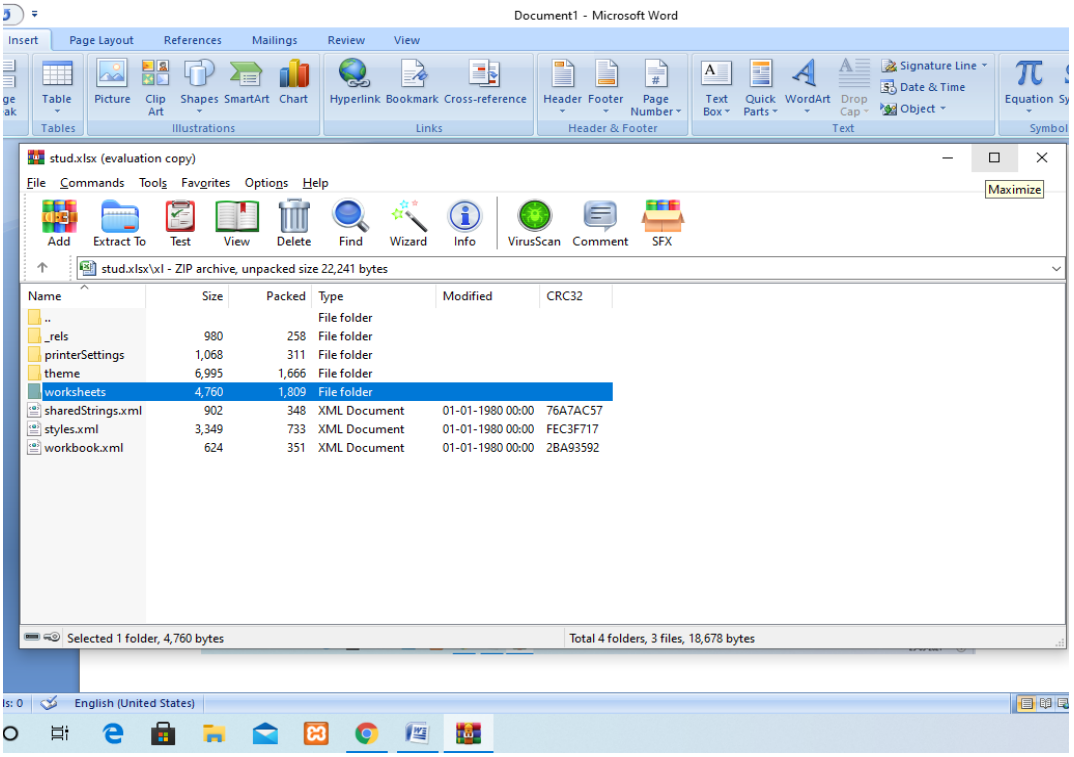
Step 10: Open the zip file by double click (or) right click and open



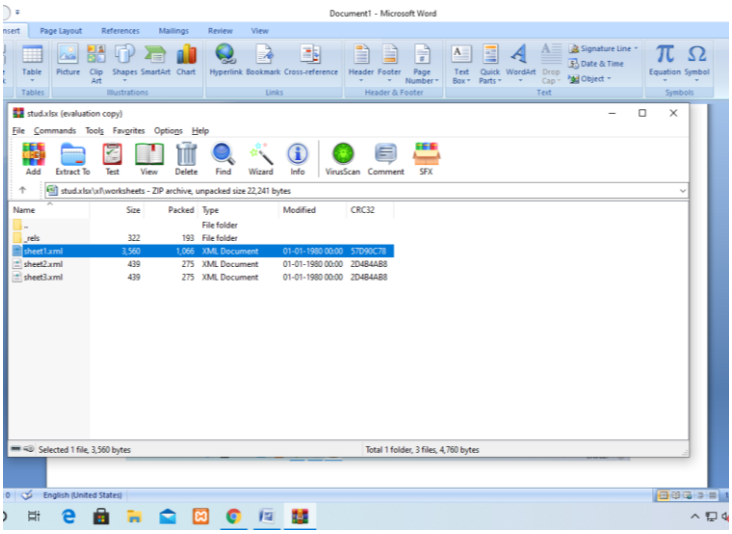
Step 11: Open the xs folder by double click (or) right click and open



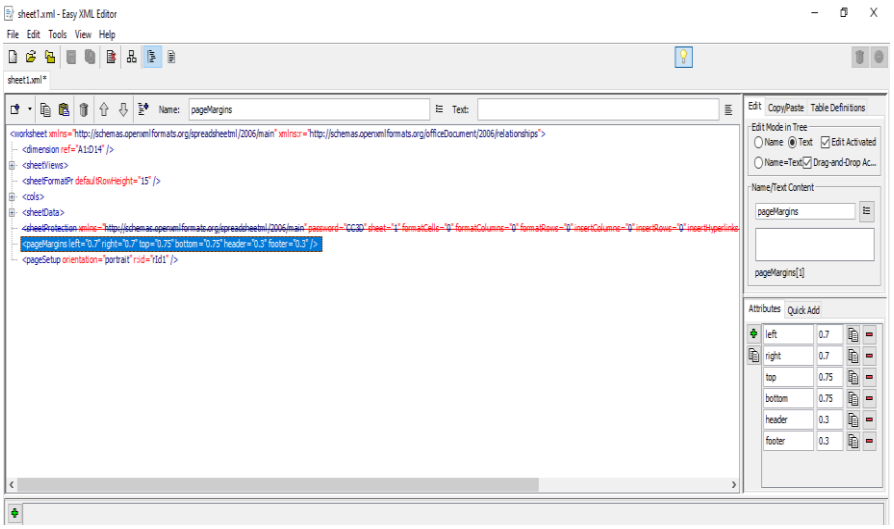
Step 12: Select the worksheet folder by double click (or) right click and open



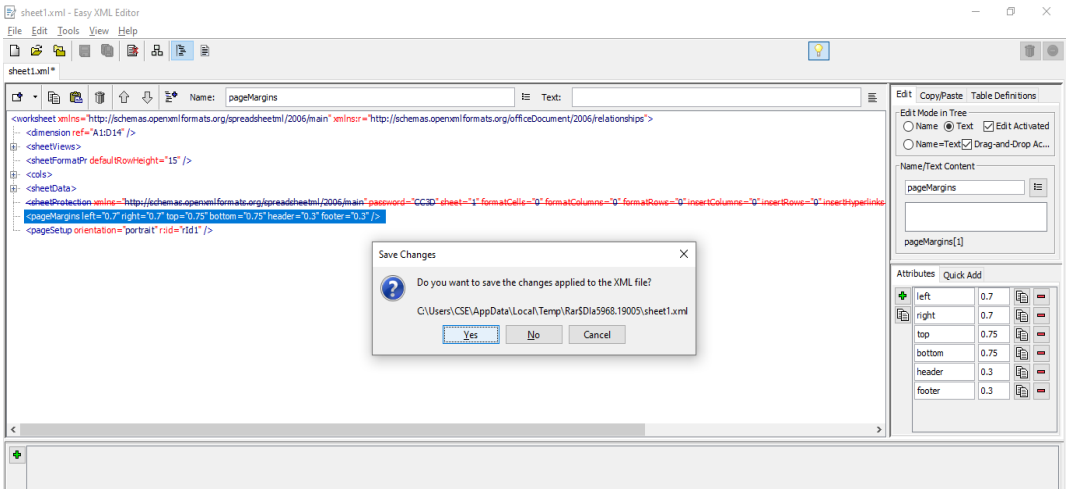
Step 13: Open the sheet1 were our official document get present



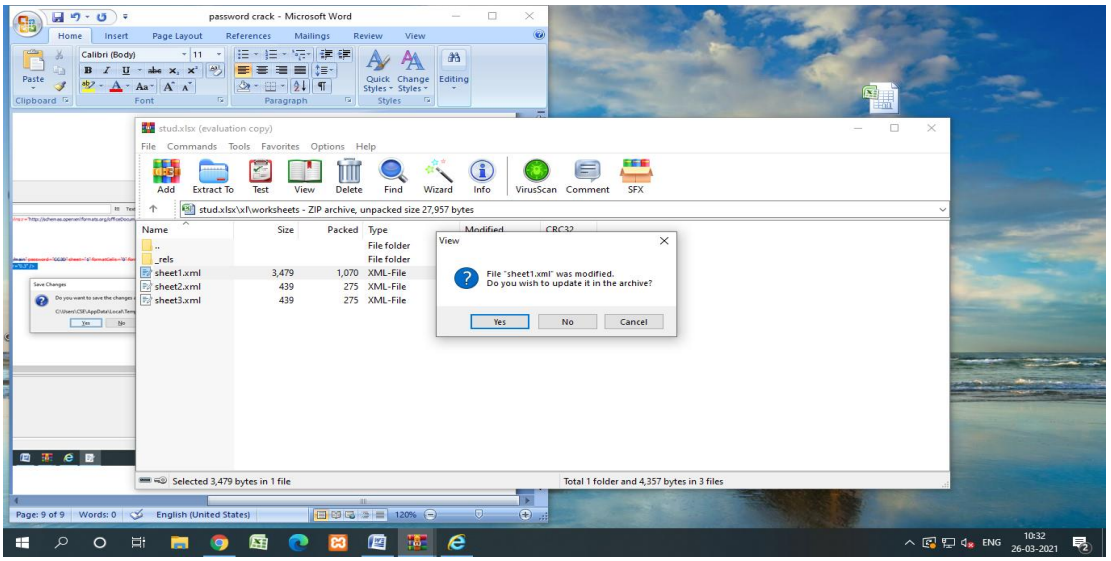
Step14: Select the password portion and delete it



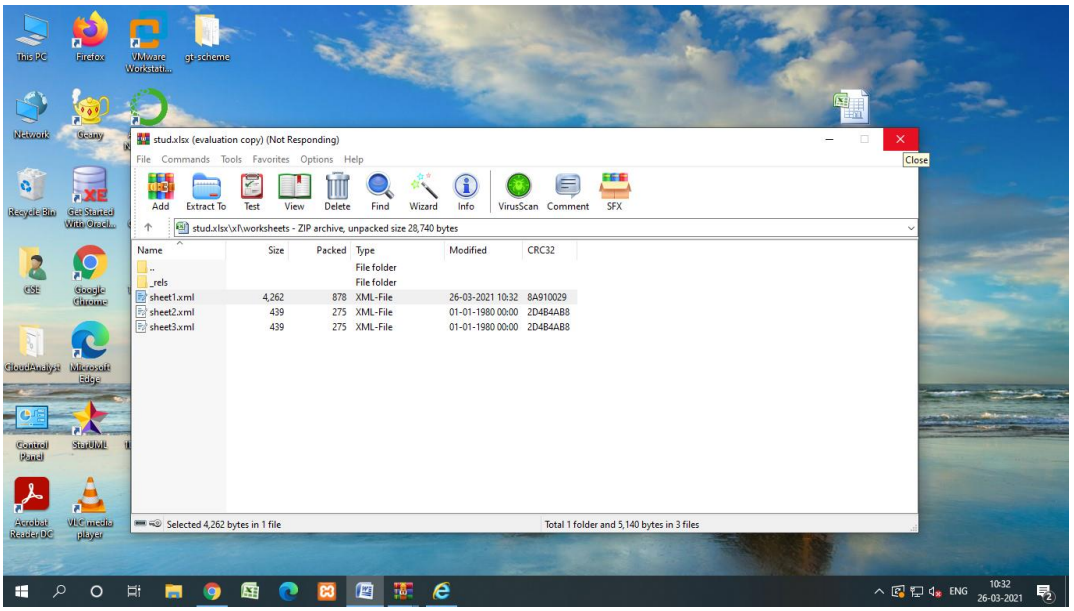
Step15: Finally save the document by selecting yes option



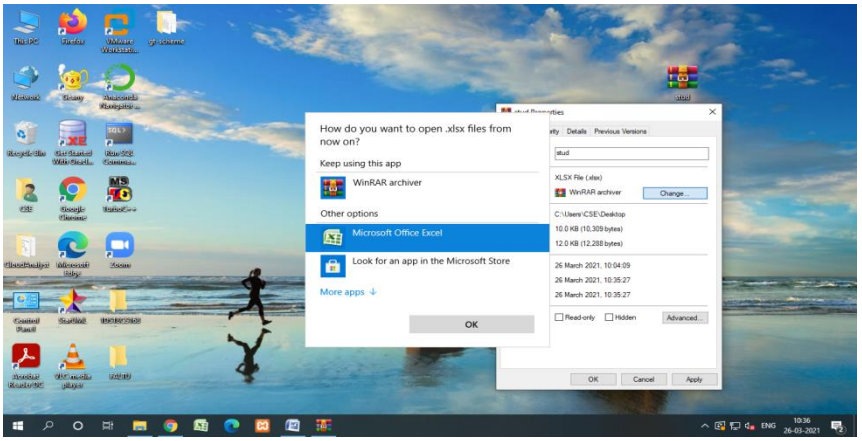
Step 16: Select yes to update the changes in the file



Step 17: Close the entire tab

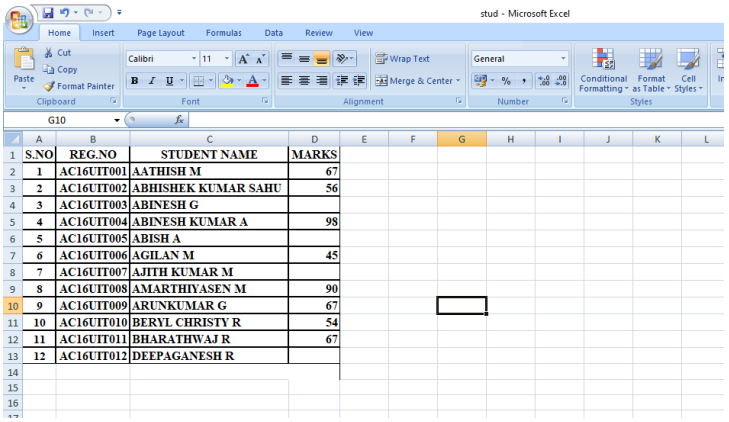


STEP 18: Again change the .zip format file to .xslx format



Step 19: The file again turned to .xslx format

Step 20: Now the document unprotected and hacker can able to edit the official data



S.NO	REG.NO	STUDENT NAME	MARKS
1	AC16UIT001	AATHISH M	67
2	AC16UIT002	ABHISHEK KUMAR SAHU	56
3	AC16UIT003	ABINESH G	
4	AC16UIT004	ABINESH KUMAR A	98
5	AC16UIT005	ABISH A	
6	AC16UIT006	AGILAN M	45
7	AC16UIT007	AJITH KUMAR M	
8	AC16UIT008	AMARTHIYASEN M	90
9	AC16UIT009	ARUNKUMAR G	67
10	AC16UIT010	BERYL CHRISTY R	54
11	AC16UIT011	BHARATHWAJ R	67
12	AC16UIT012	DEEPAGANESH R	

RESULT:

The main aim is to open an authorized ms excel document by password cracking is completed successfully.

EXPT.NO 2(B)	SCANNING THE SYSTEM VULNERABILITIES USING MICROSOFT BASELINE SECURITY ANALYZER (MBSA) TOOL	DATE:

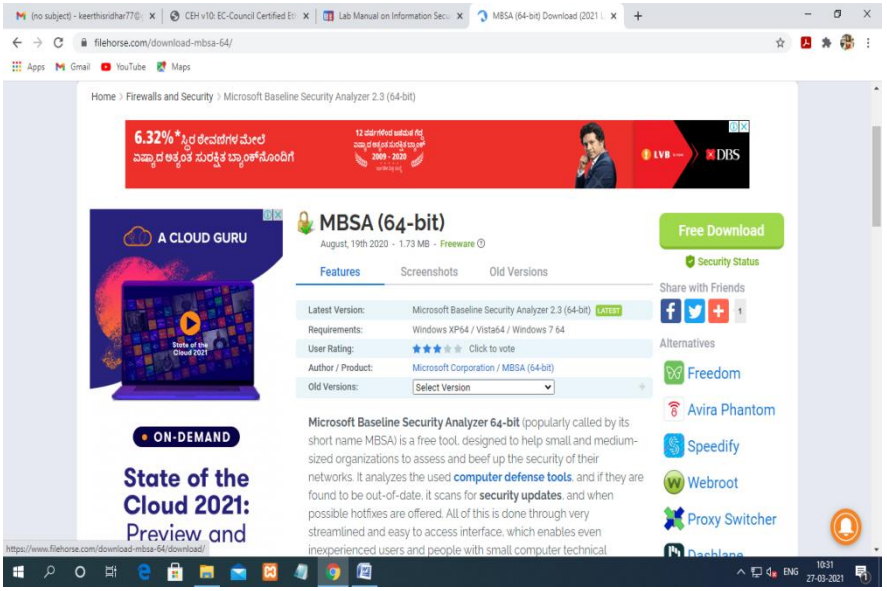
AIM:

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

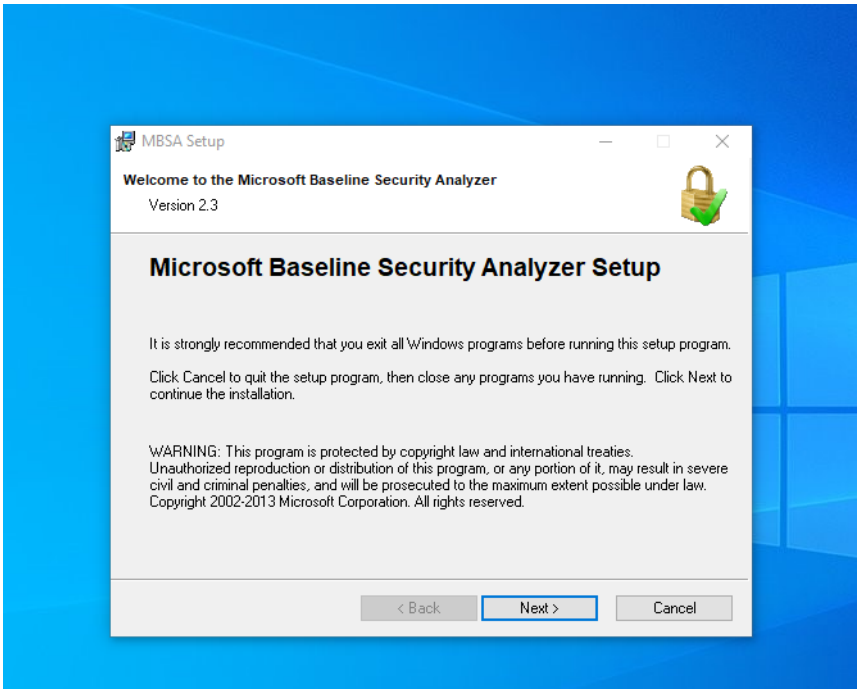
PROCEDURE:

- **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.**

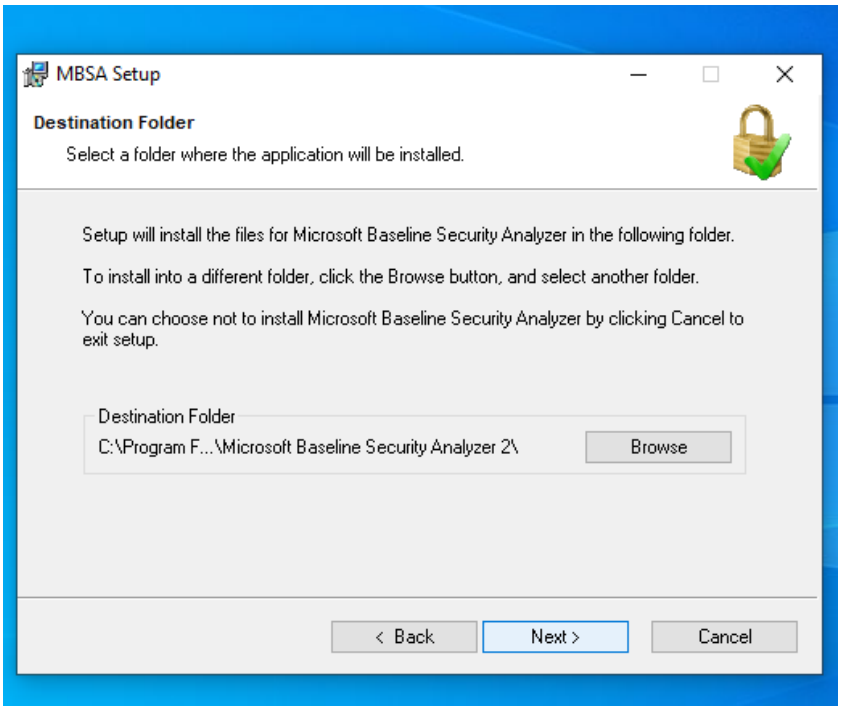
Step 1: download the Microsoft Baseline Security Analyzer (MBSA)



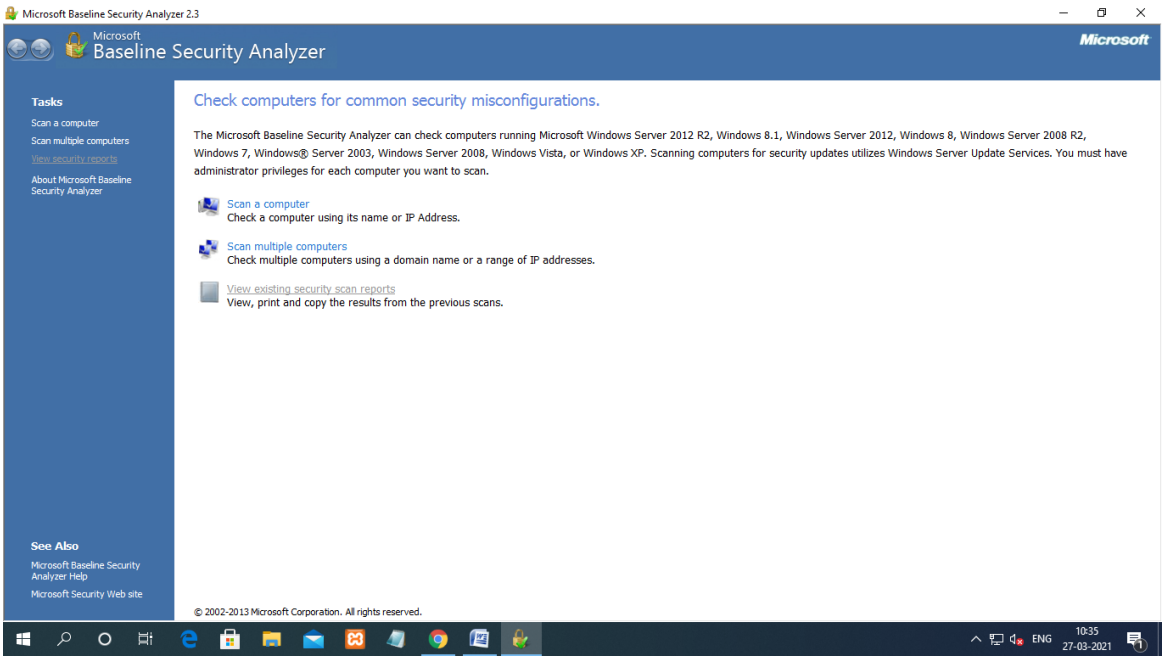
Step2: start and install the Microsoft Baseline Security Analyzer (MBSA) click next to start install



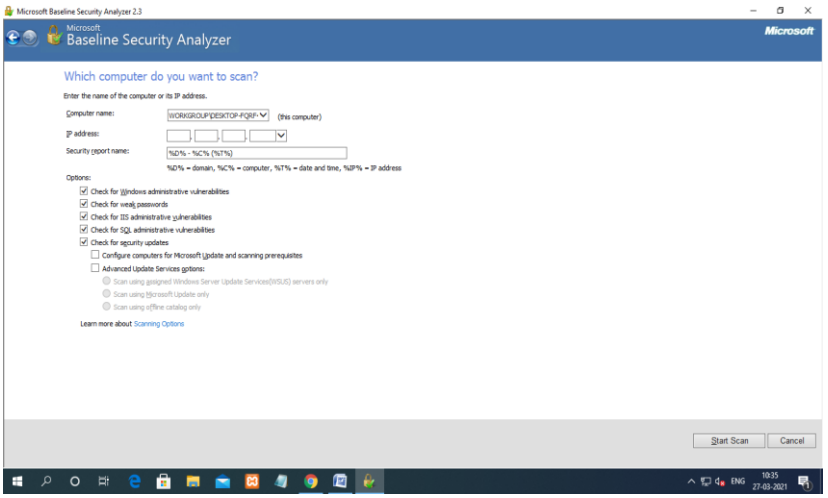
Step3: choose the location to install MBSA



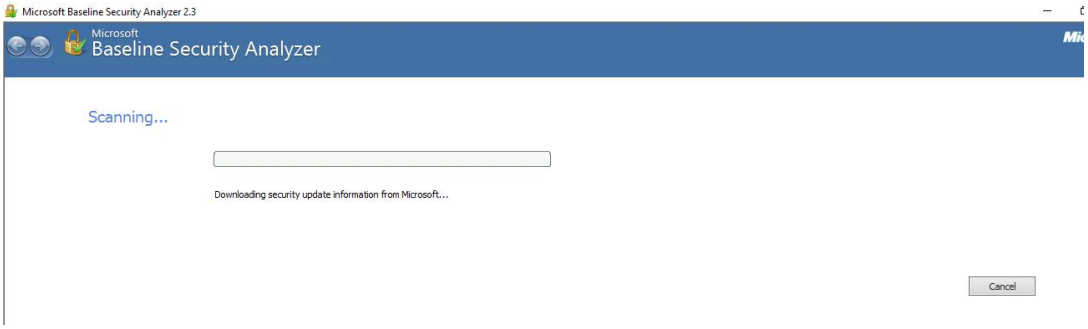
STEP 4:click the scan a computer to start the MBSA



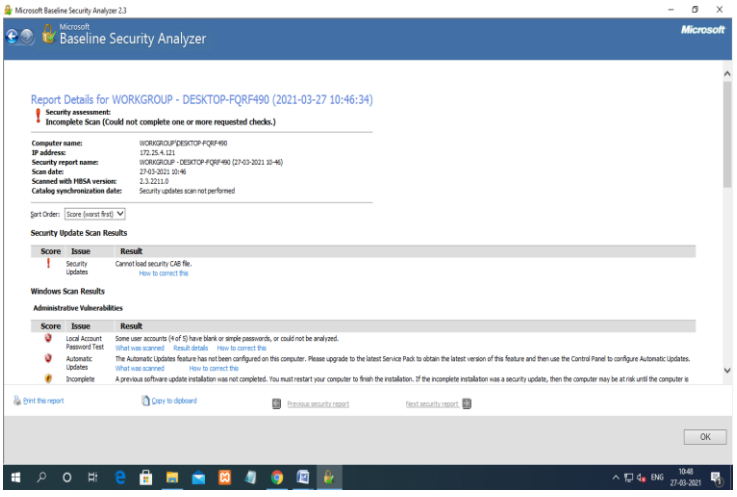
Step 5: provide the IP address and click start scan



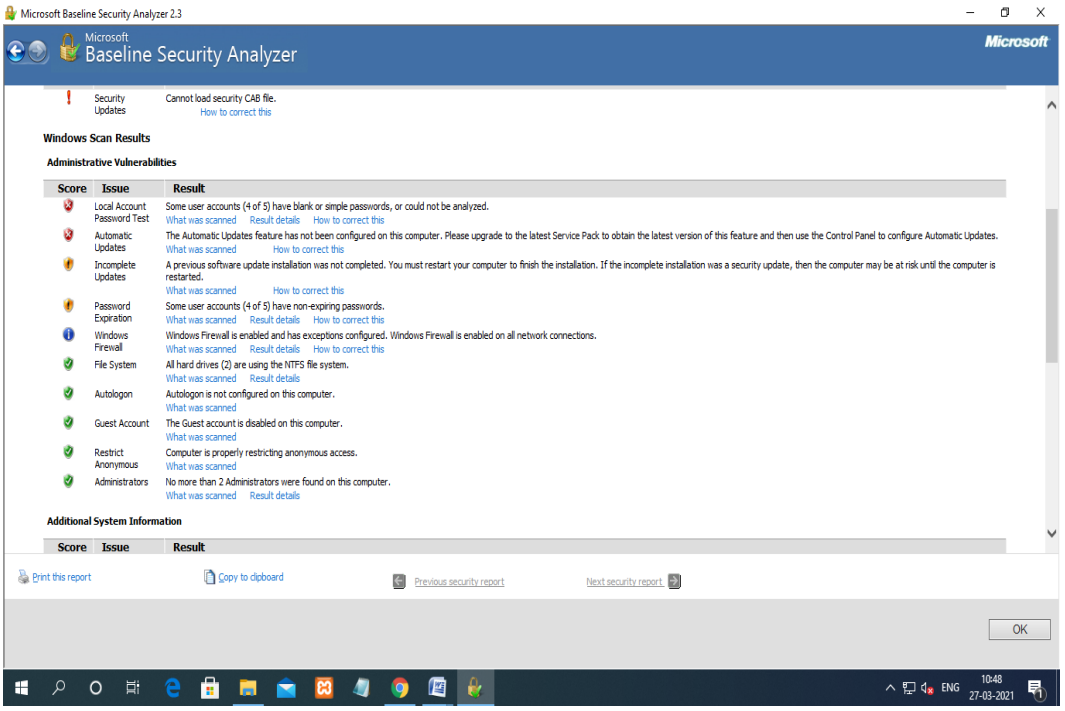
Step 7: The scanning process is GET STARTED



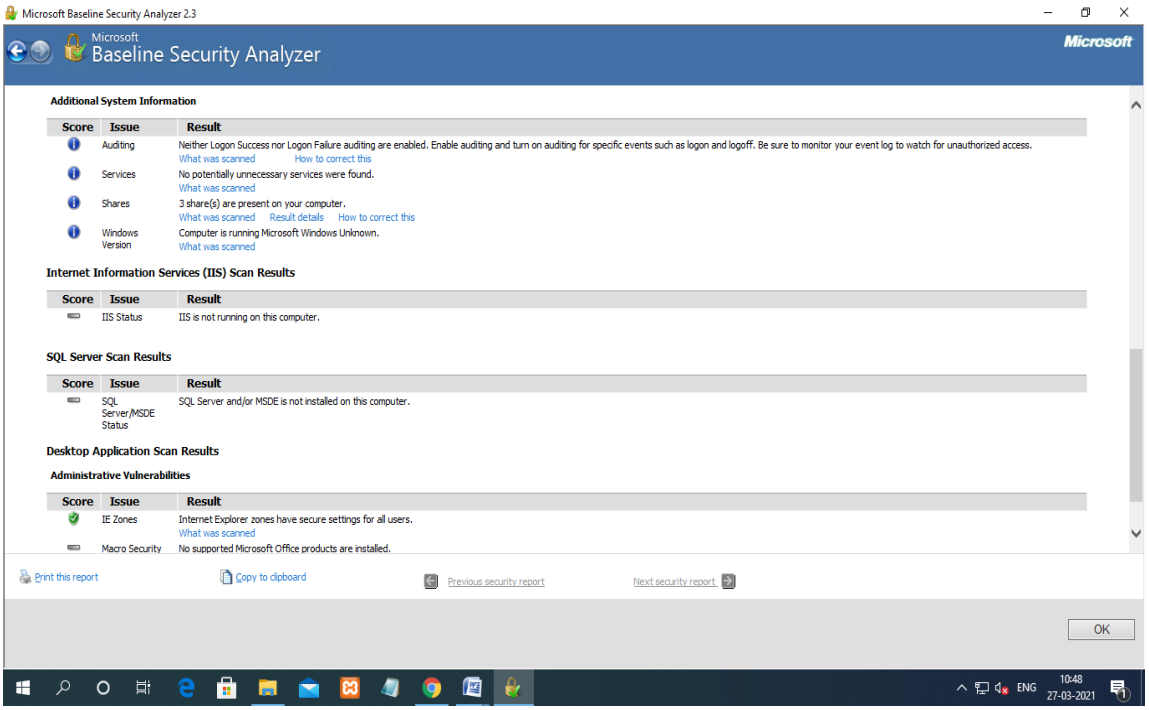
STEP 8: The detail report is generated for the system



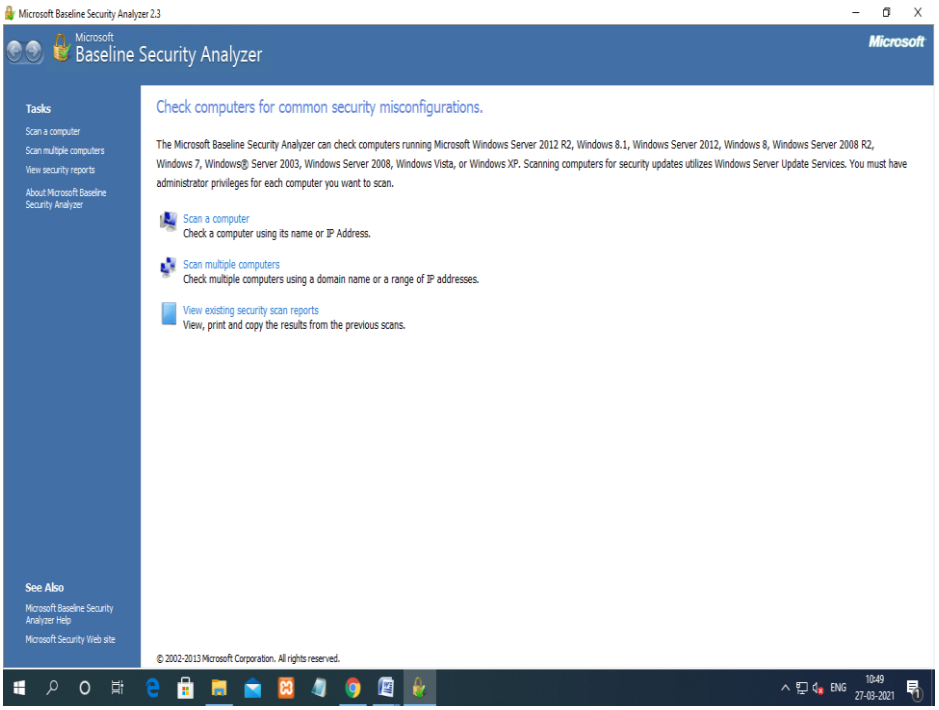
Result about the administrative vulnerabilities



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 baseline security analyzer (MBSA) **is completed successfully.**

EXPT.NO 3(a)	Study of Cyber Forensic Tools.	DATE:

EXPT.NO 3(B)	COMPARISON **OF** TWO FILES FOR FORENSICS INVESTIGATION BY COMPARE IT TOOL	DATE:

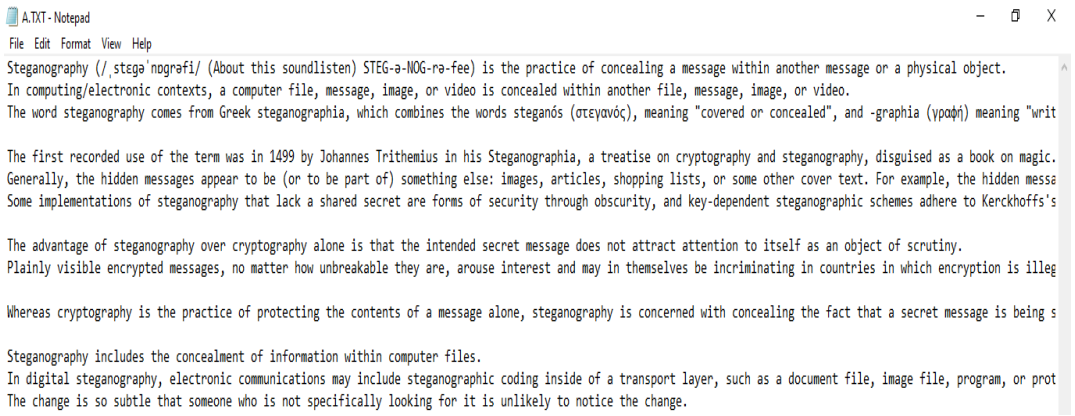
AIM:

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

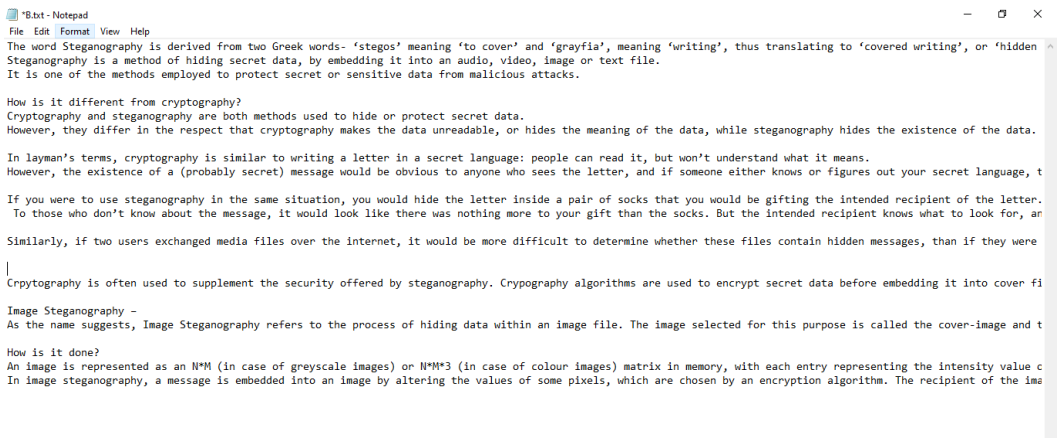
PROCEDURE:

- **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. First of 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 save with a file name

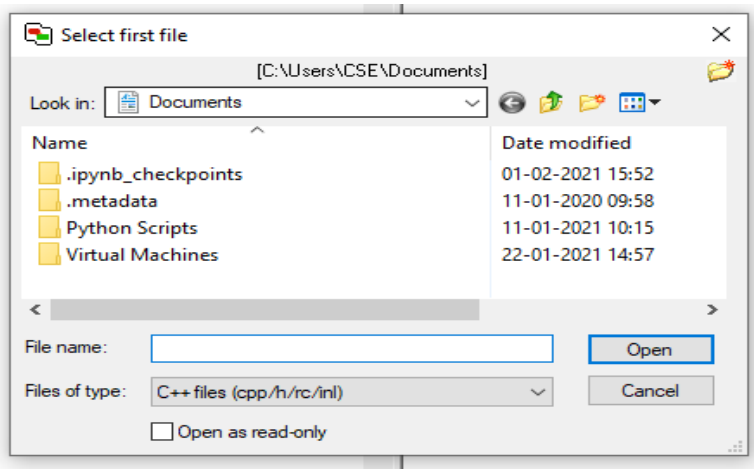


Step 2: create a second text file with the extension .txt

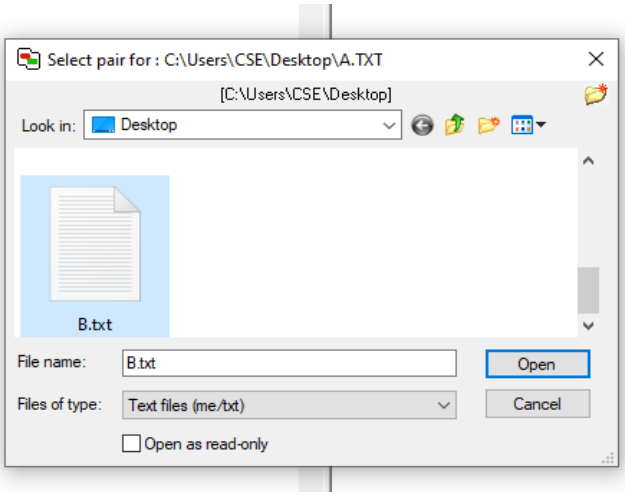


Step 4: Download the compare it tool install the Compare It from the Link given below. http://www.grigsoft.com/wincmp3.htm it is a 1.7 Mb Software package Click on Compare It Tool, It will show a window to select the files to be compared.

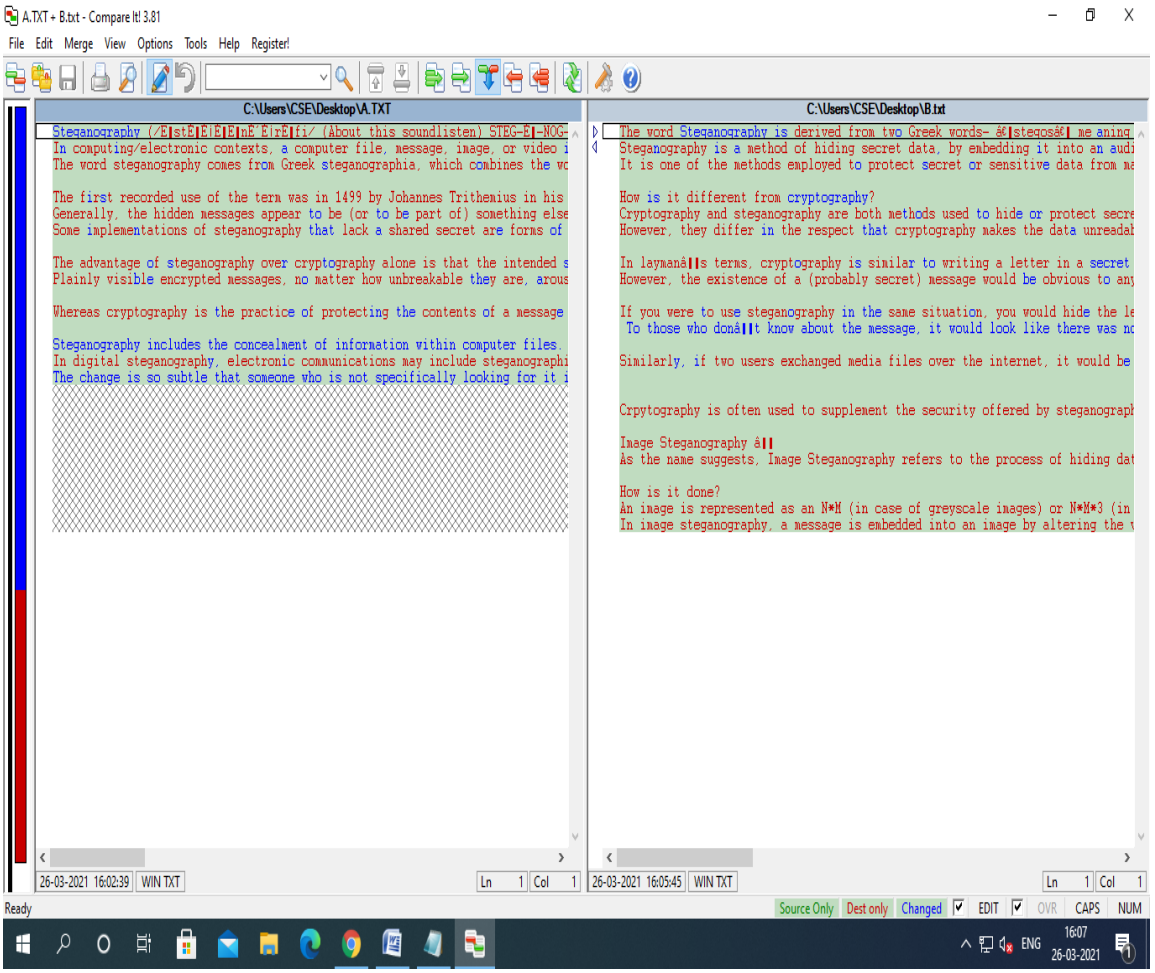
Step 5: Upload the first file to the compare it tool



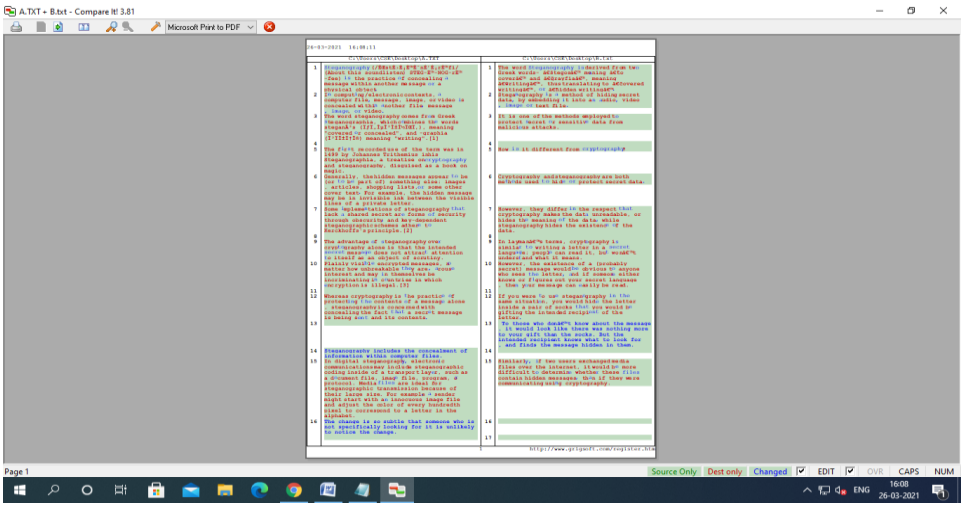
Step 6: upload the second file to the compare it tool



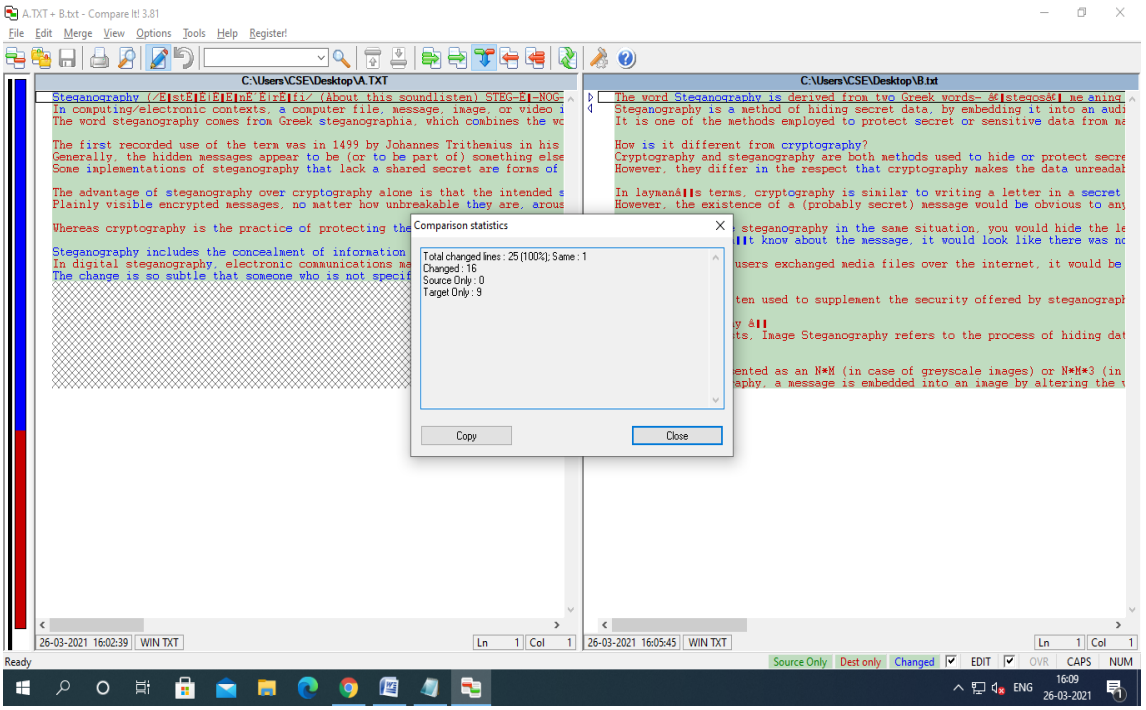
Step 7: Displays 2 files side by side, with colored differences sections to simplify analyzing. You can move changes between files with a single mouse click or keystroke



STEP 8: It also gives you Print report of the difference in the file as follows



STEP 9: the comparison result is get display.



RESULT:

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

EXPT.NO 4(A)	Analyze the Port vulnerability of the system using NMAP to ensure security in Apache Server	DATE:

AIM:

The main aim is to scan the port using nmap in Apache server.

PROCEDURE:

NMAP Tool:

Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan.

Nmap features include:

- **Host discovery – Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.**
- **Port scanning – Enumerating the open ports on target hosts.**
- **Version detection – Interrogating network services on remote devices to determine application name and version number.**
- **TCP/IP stack fingerprinting – Determining the operating system and hardware characteristics of network devices based on observations of network activity of said devices.**
- **Scriptable interaction with the target – using Nmap Scripting Engine[1] (NSE) and Lua programming language.**

STEP 1 : Start the Virtual Machine and launch Kali Linux.

STEP 2 : open the terminal

STEP 3 : Stop the previously running Apache server (if any) using the code

```
sudo systemctl stop apache2
```

```
File  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/kali]
└─# sudo systemctl stop apache2
```

STEP 4 : Now, using the following code, start the Apache server.

sudo systemctl start apache2

```
┌──(root㉿kali)-[/home/kali]
└─# sudo systemctl start apache2
```

STEP 5 : Use NMAP to scan the current working system's IP address for any open ports.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.168.131
```

STEP 6 : Analyze the output and the services that are running on that IP address.

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-06 03:19 EST
Nmap scan report for 192.168.168.131
Host is up (0.0000060s latency).
Not shown: 994 closed tcp ports (reset)
PORT   STATE SERVICE
20/tcp open  ftp-data
21/tcp open  ftp
22/tcp open  ssh
25/tcp open  smtp
53/tcp open  domain
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

STEP 7 : Close the Apache server using the code below.

sudo systemctl stop apache2

RESULT:

The main aim is to scan the port using nmap in Apache server is successfully completed.

EXPT.NO 4(B)	STEGANOGRAPHY - HIDING AND RECOVERING THE INFORMATION USING QUICKSTEGO TOOL	DATE

AIM:

The main aim is to hide and recover the information using QUICKSTEGO TOOL.

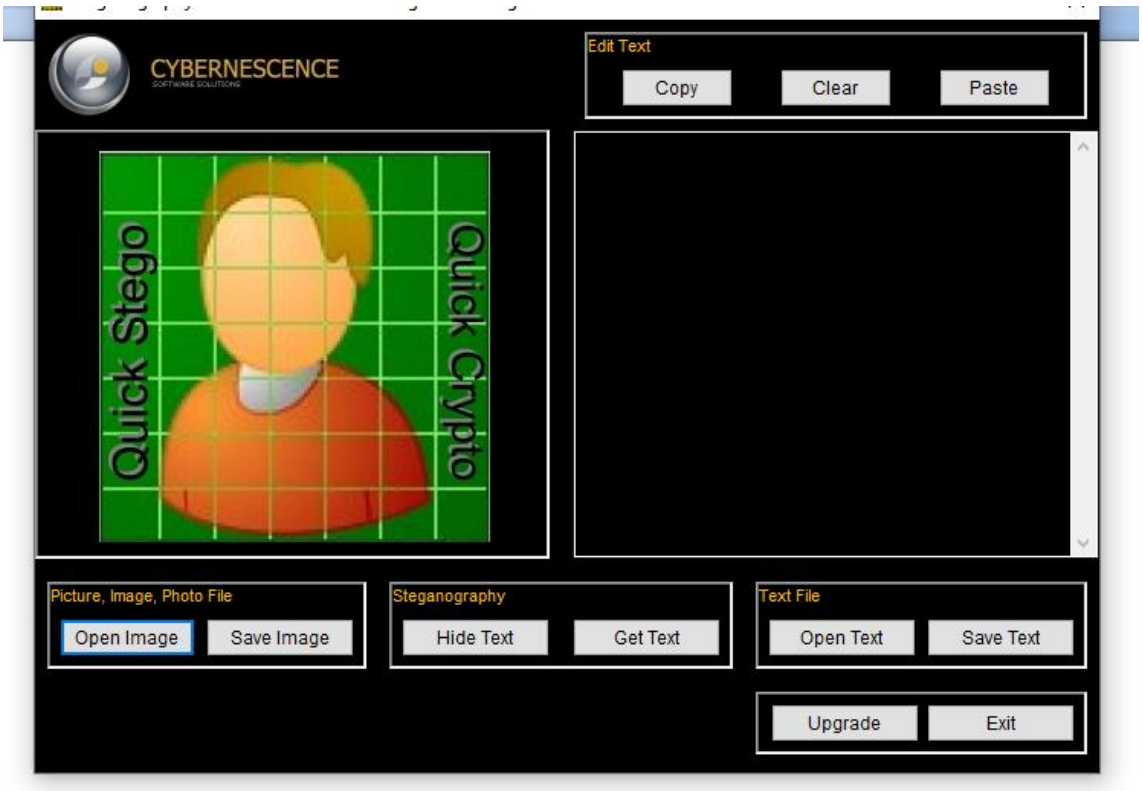
PROCEDURE:

- **Steganography is the science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message.**
- **QuickStego lets you hide text in pictures so that only other users of QuickStego can retrieve and read the hidden secret messages. Once text is hidden in an image the saved picture is still a 'picture', it will load just like any other image and appear as it did before.**

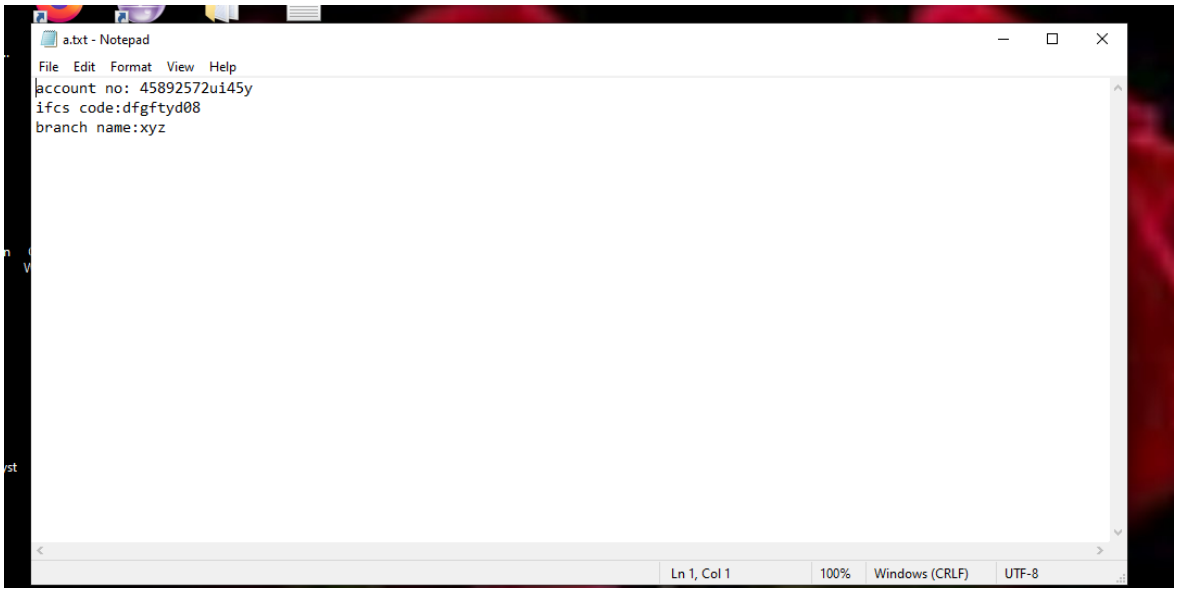
Step 1 : Download the QuickStego tool

Step 2 : Install the QuickStego tool and launch the desktop icon

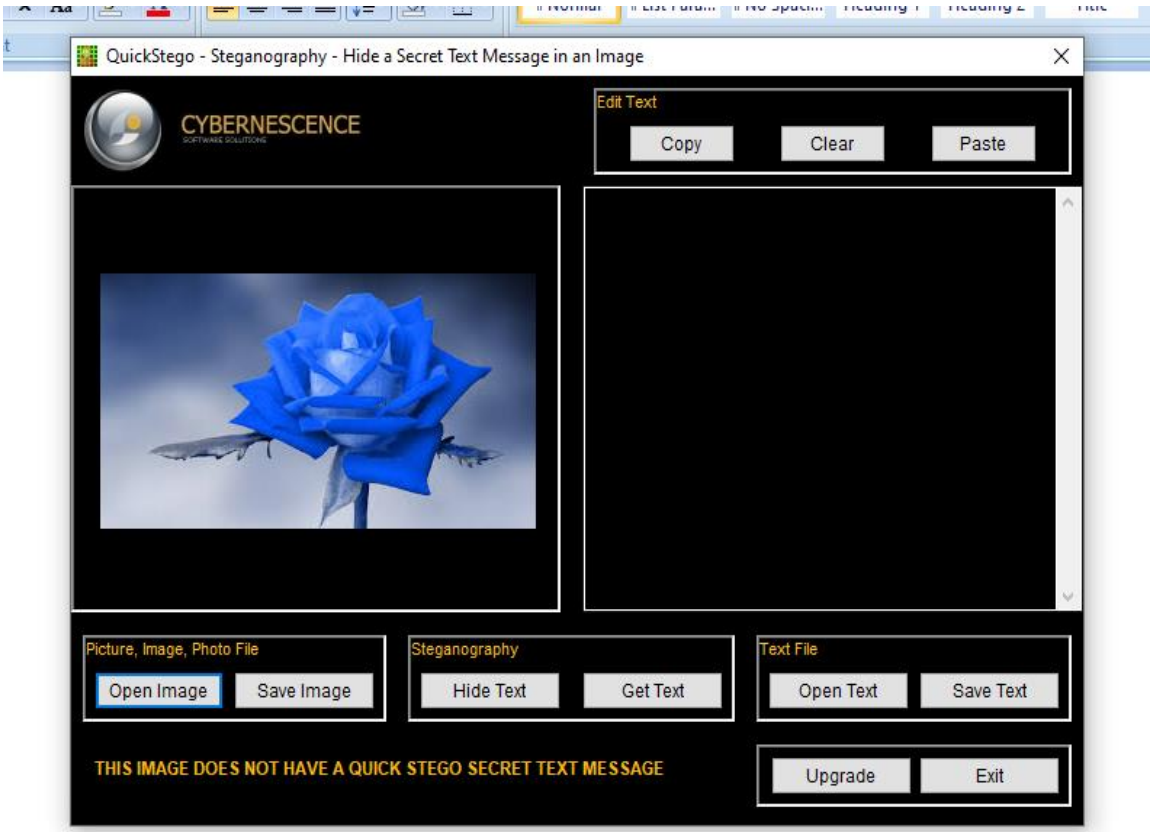
Step 3 : Open the QuickStego application



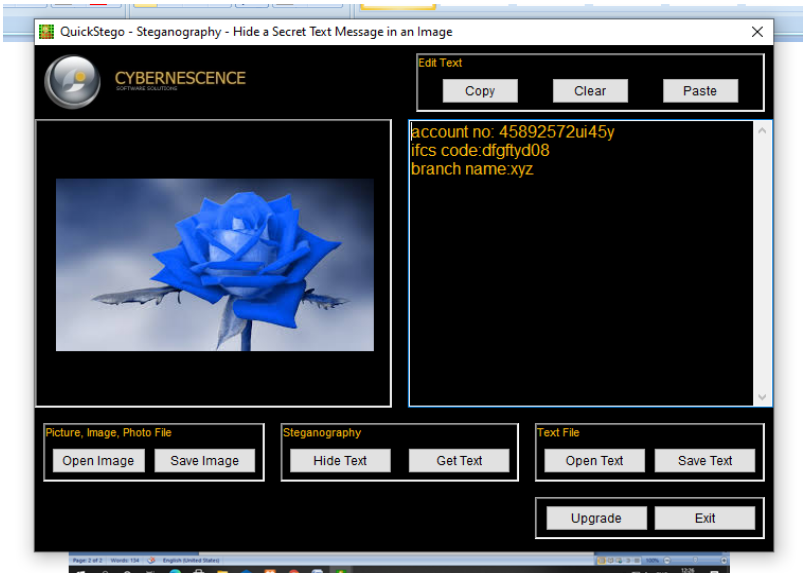
Step 4 : Create a text file or otherwise directly we can give the text data here we are creating a secrete text file with the extension .txt to upload in the image



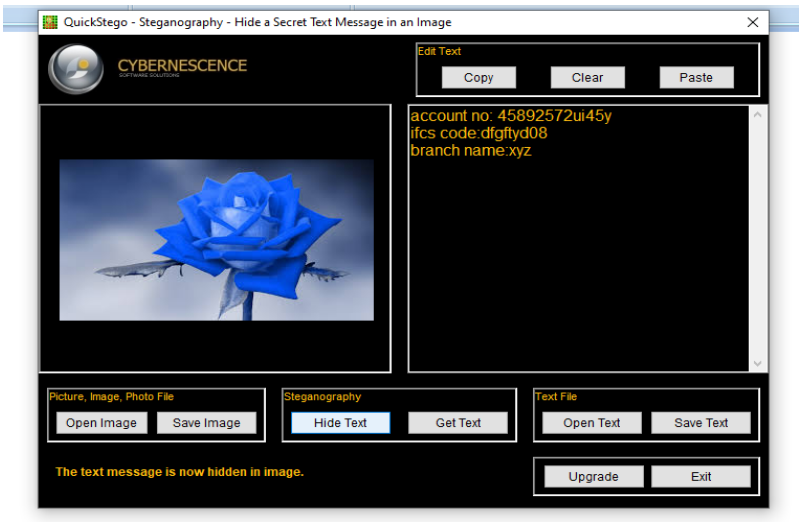
Step 5 : upload the image file to the QuickStego application



Step 6: Upload the text file to the QuickStego application



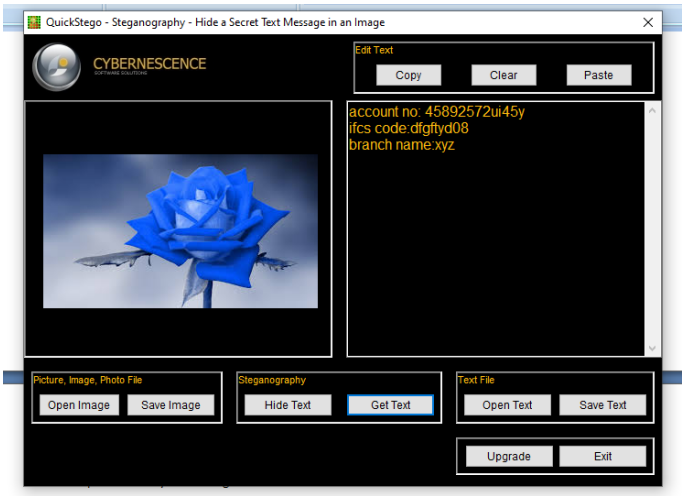
Step 7 : Click hide text to hide the text document to image



Step 8 : Click save image to upload the secret data to image a new image file is created and saved

Step 9: Now close the stego application and open it again

Step 10 : Now open the newly saved image and click the Get Text



RESULT:

The main aim is to hide and recover the information using QUICKSTEGO TOOL is completed successfully.

EXPT.NO 5(a)	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 :

hhhhhhhhhhhhhhhhhhhh

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 5(b)	Implement a versatile hacking tool - Hashcat Tool for cracking the password.	

AIM:

The main aim is to crack the password using Hashcat Tool

PROCEDURE:

Hashcat is a password cracking tool used for licit and illicit purposes.

Hashcat is a particularly fast, efficient, and versatile hacking tool that assists brute-force attacks by conducting them with hash values of passwords that the tool is guessing or applying

It gives the user the ability to brute-force credential stores using known hashes, to conduct dictionary attacks and rainbow tables, and to reverse engineer readable information on user behavior into hashed-password combination attacks.

It supports a wide range of hashing algorithms including MD5, SHA-1, SHA-2, and more. Hashcat works by using the power of a computer's GPU to test millions of passwords per second. It can also utilize multiple GPUs or even cluster-based processing for even faster password cracking.

Step1 **: Open the hash file with the cat command, which will display the hash**

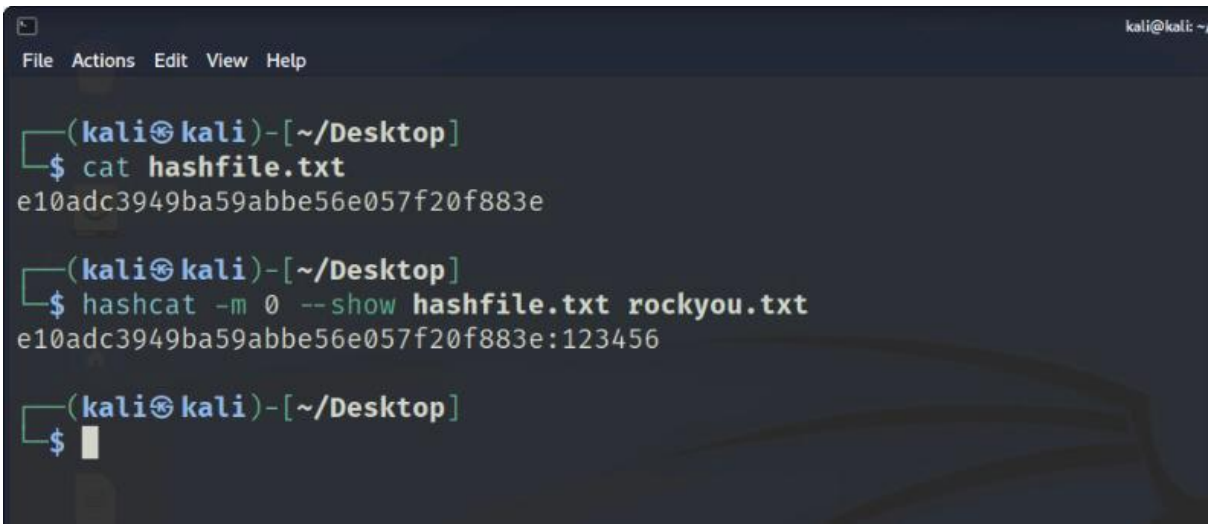
Cat file.txt

Step 2: **Use the hashcat tool to crack the password.**

NOTE: **For this you will need a file for a dictionary attack to perform brute force Credential check.**

Step 3: **write the following command for crackin g the password using hash**

Hashcat -m 0 hashfile.txt rockyou.txt



NOTE : If the above command doesn't work try the following command

Hashcat -m 0 –show hashfile.txt rockyou.txt

RESULT:

The main aim to crack the password using Hashcat Tool is successful

EXPT.NO 6(A)	DOWNLOADING A WEBSITE USING WEBSITE COPIER TOOL(HTTRACK)	DATE:

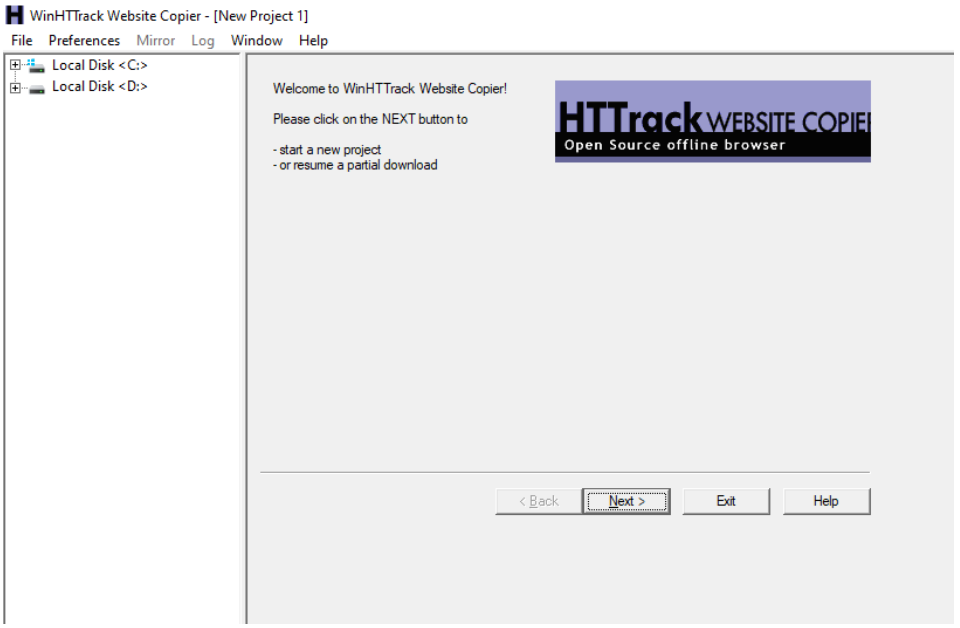
AIM:

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

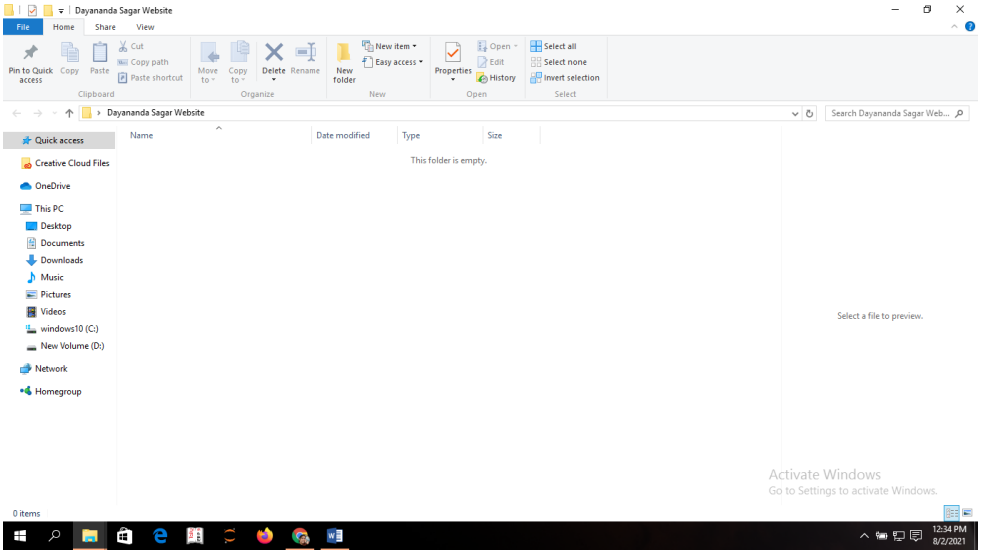
PROCEDURE:

- **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.**

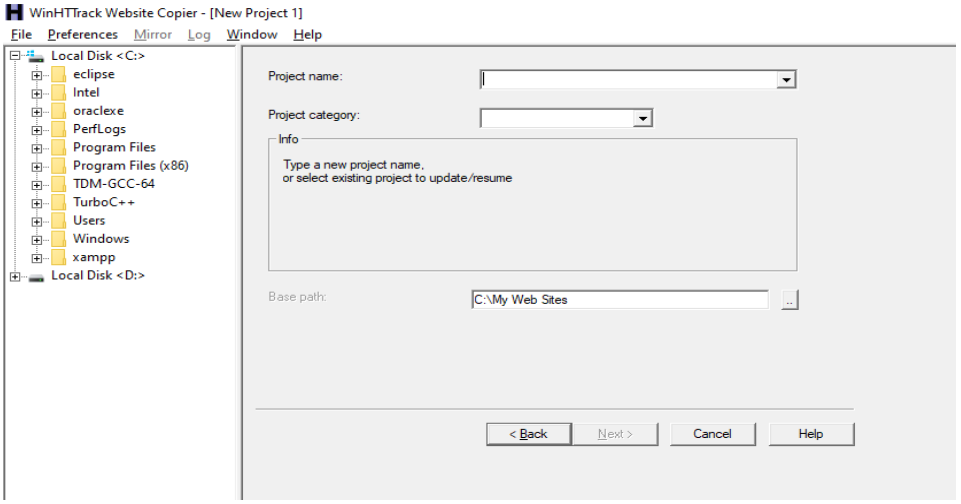
STEP 1: Install WinHTTrack



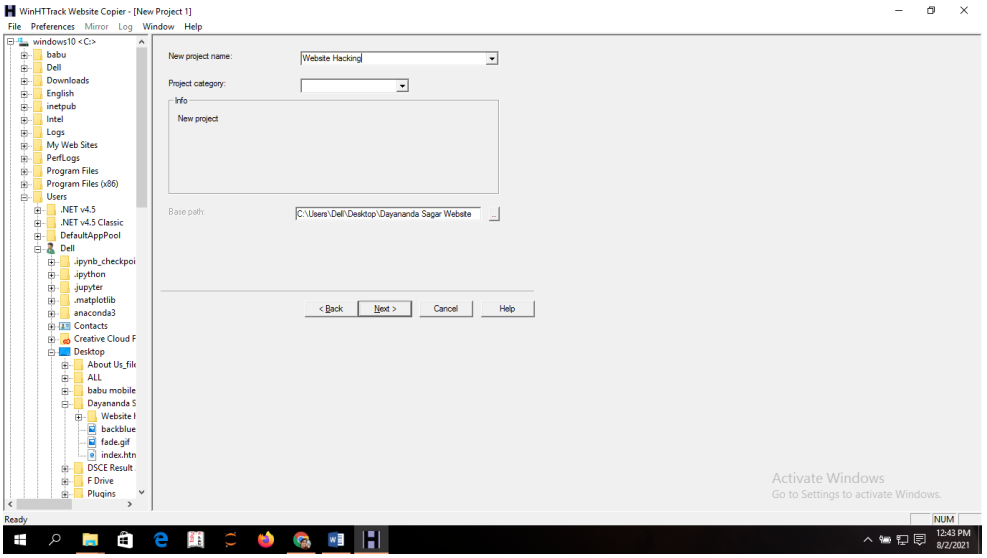
STEP 2: Create a folder on the Desktop and rename the folder name.
For Example: Folder name is “Dayananda Sagar Website”.
Open the folder “Dayananda Sagar Website”. The content of the folder is empty.



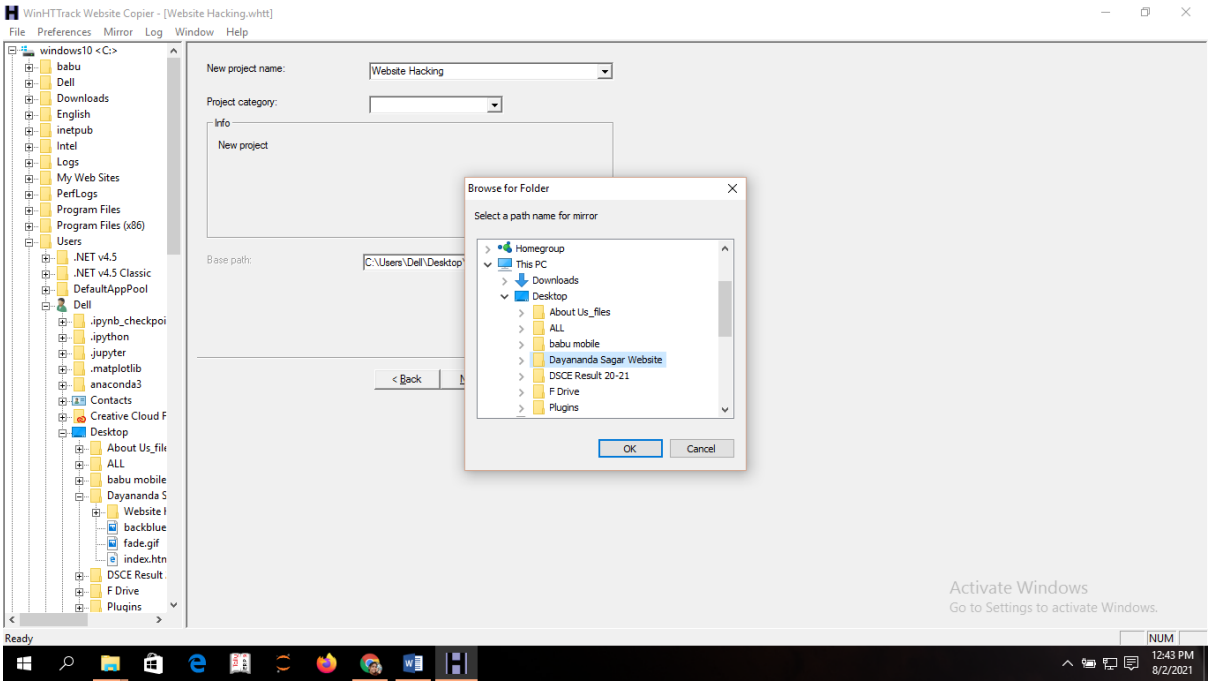
STEP 3: Select the new project from the file menu.



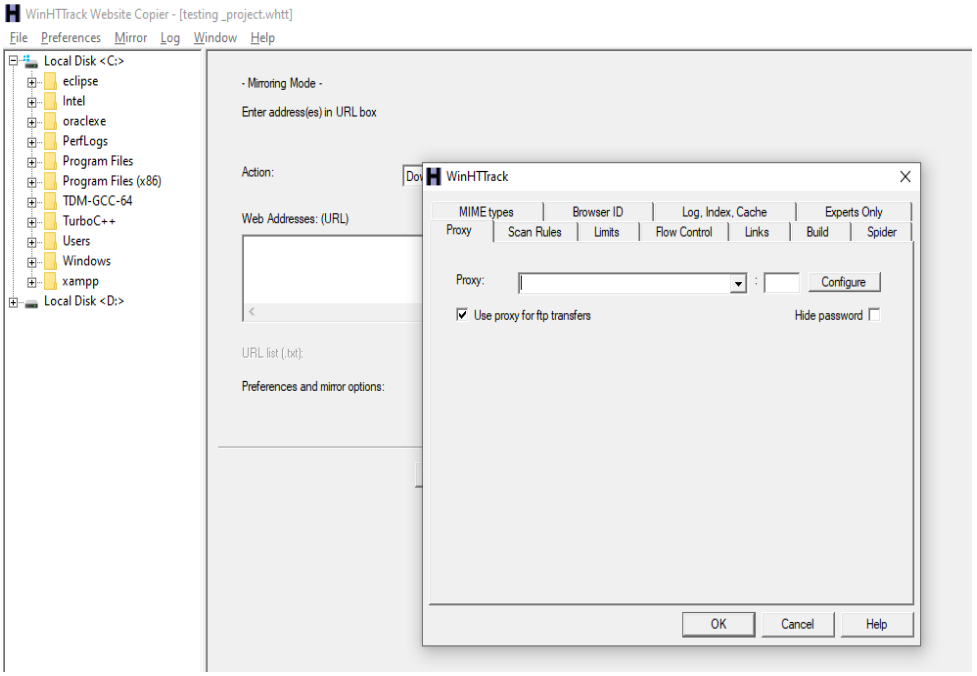
STEP 3: Enter the project name in new project field: Example: Website hacking



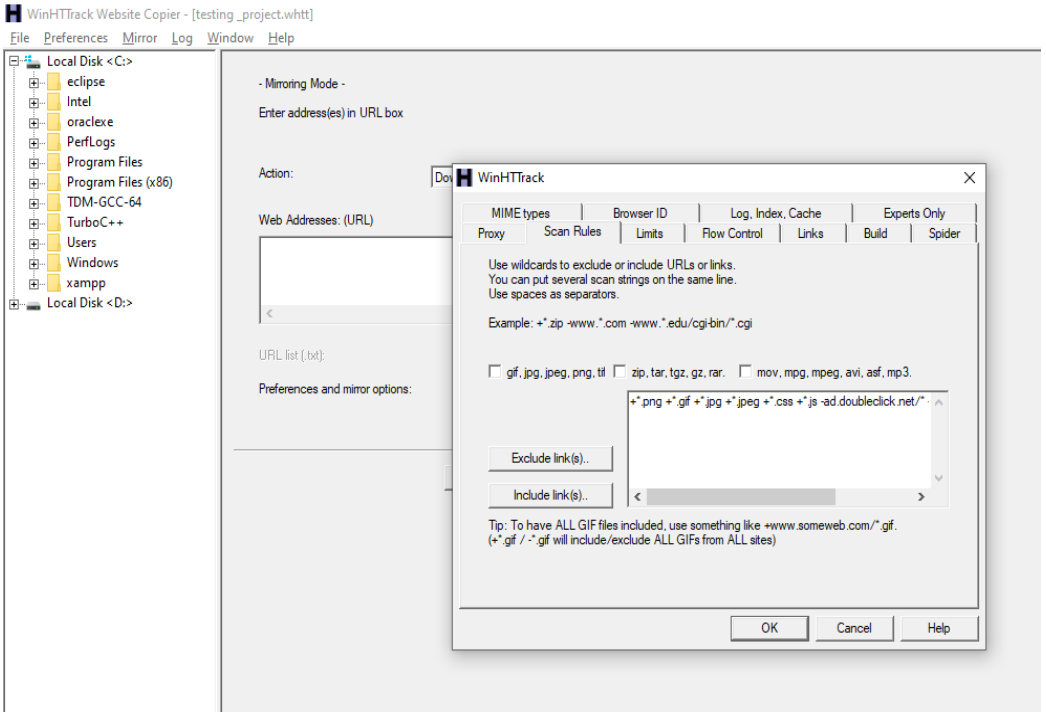
Step 4: Give the path where you need to download the files. In order to do this Click on Desktop and then click the folder "Dayananda Sagar Website". Press OK



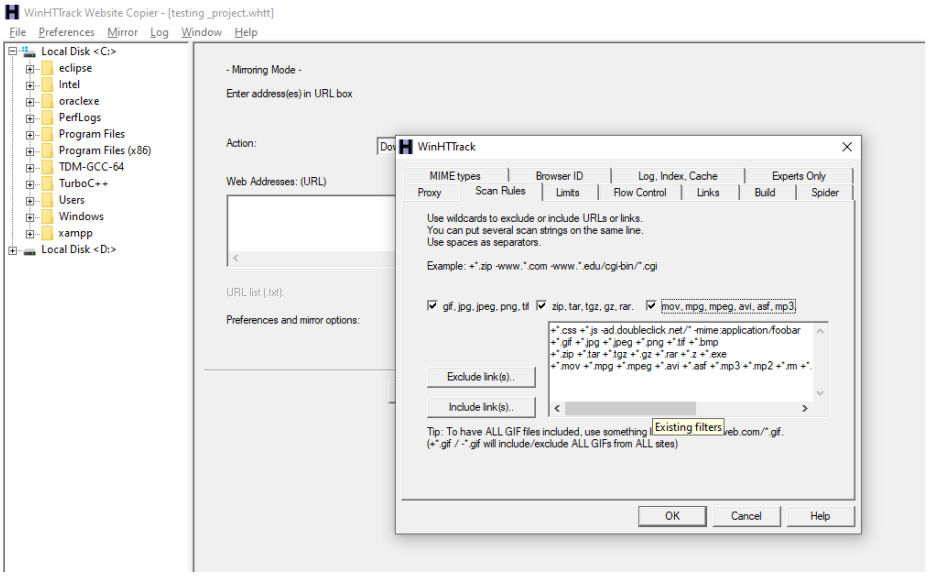
Step 5: **WinHTTrack option window is opened select the scan rules**



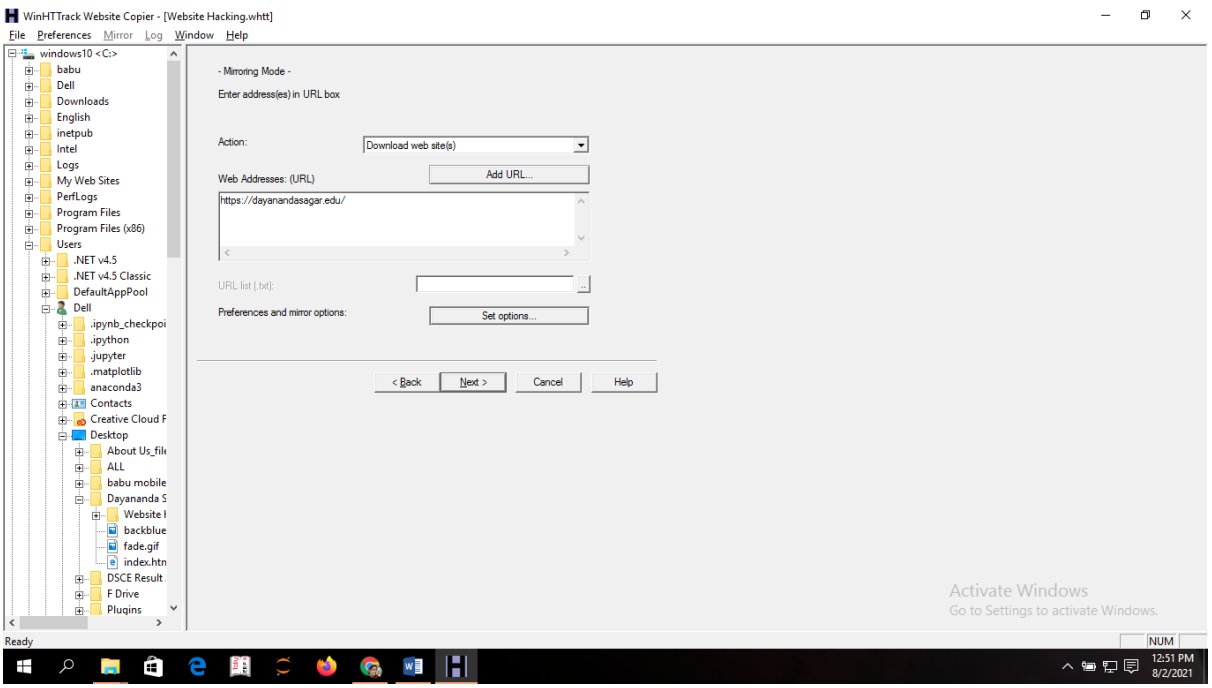
Step 6: Select all type of file to start the scan.



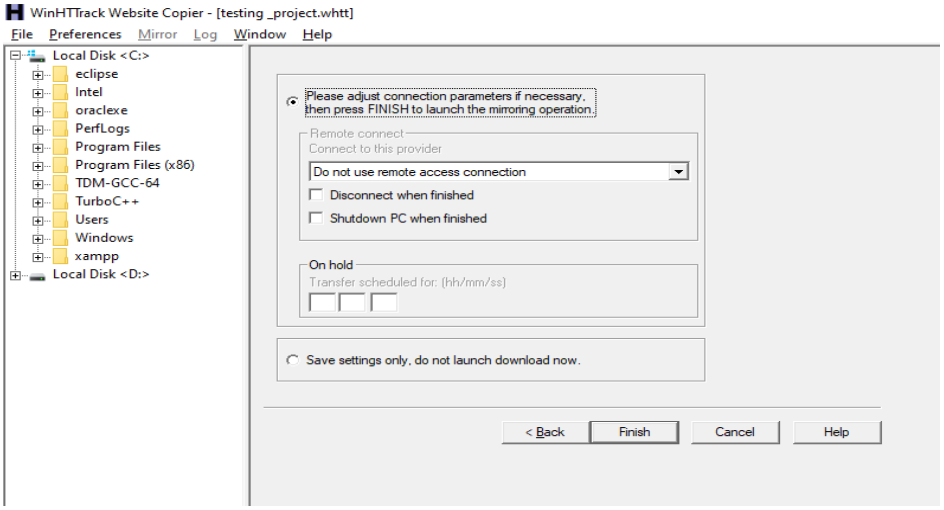
Step 7: Now all the extension is added for the scan.



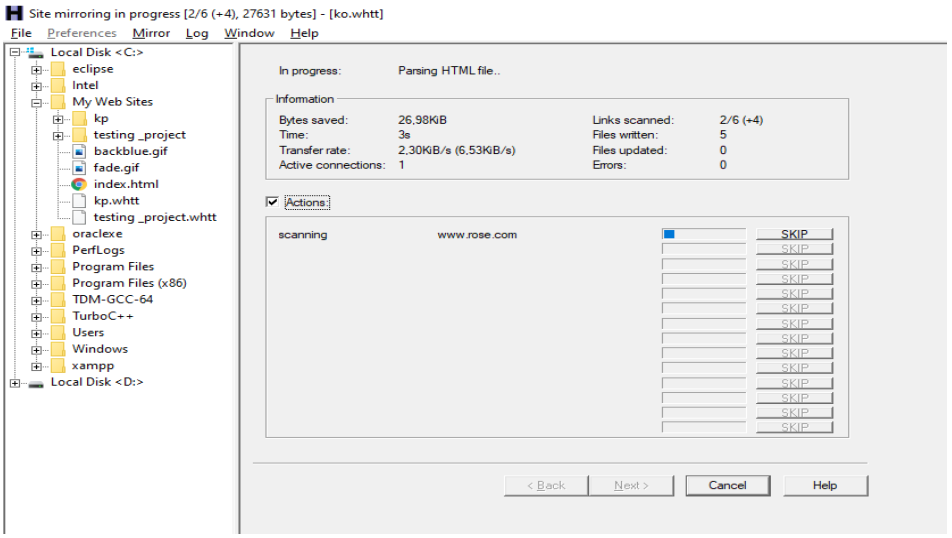
Step 8: Now type the URL address to scan



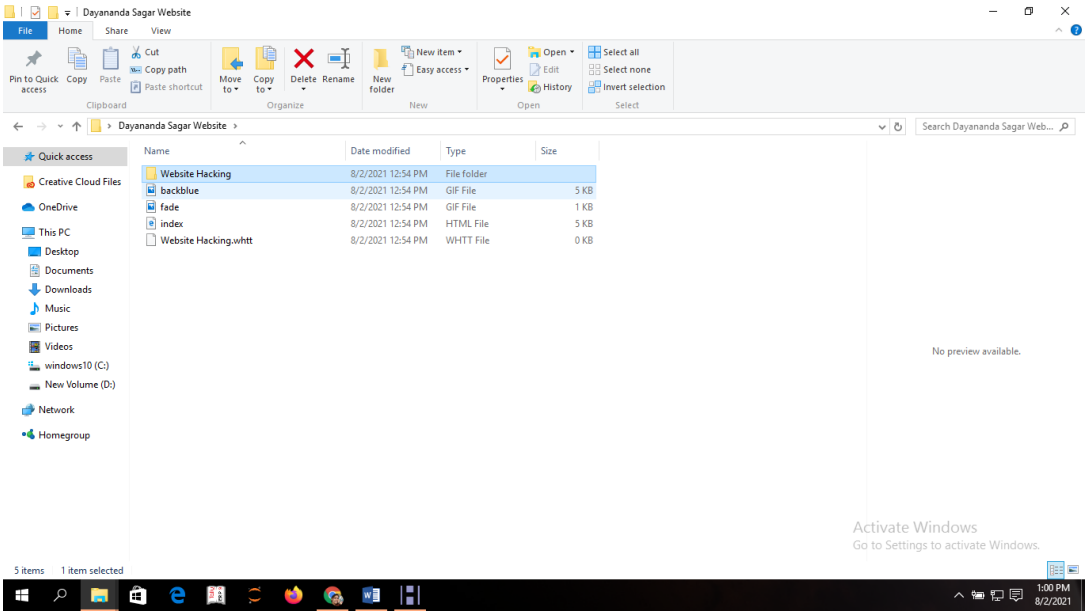
Step 9: Enable the connection adjustment if needed and click the finish button.



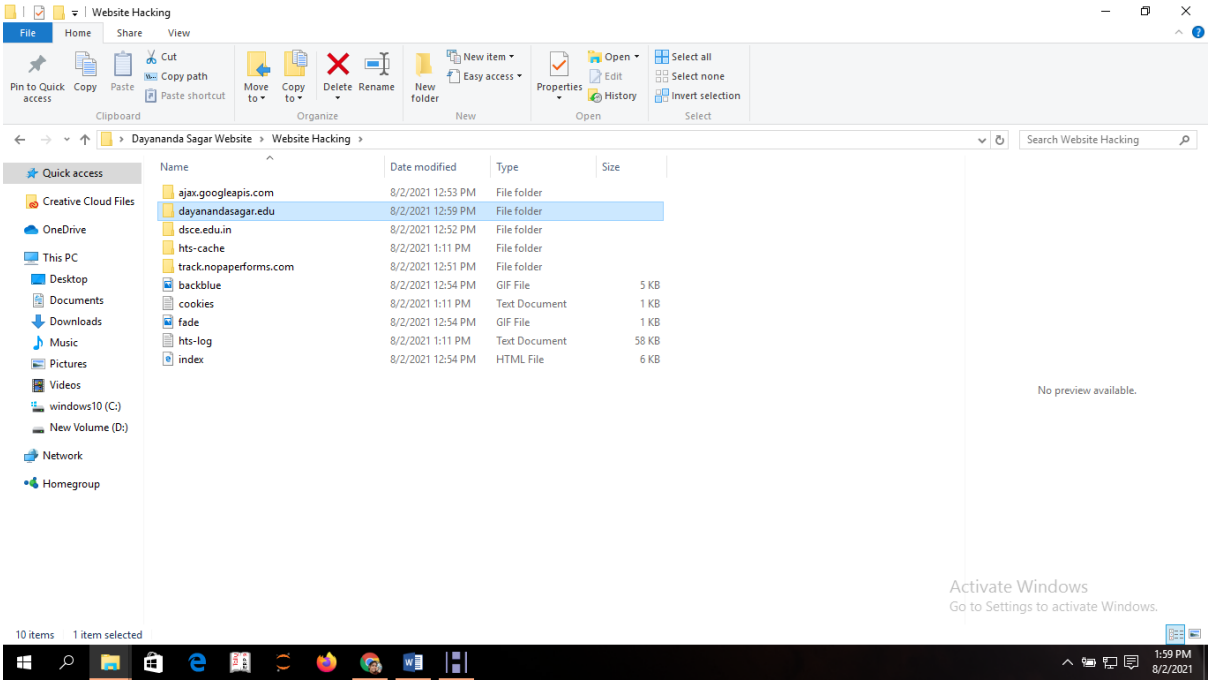
Step 10: mirroring process is get started



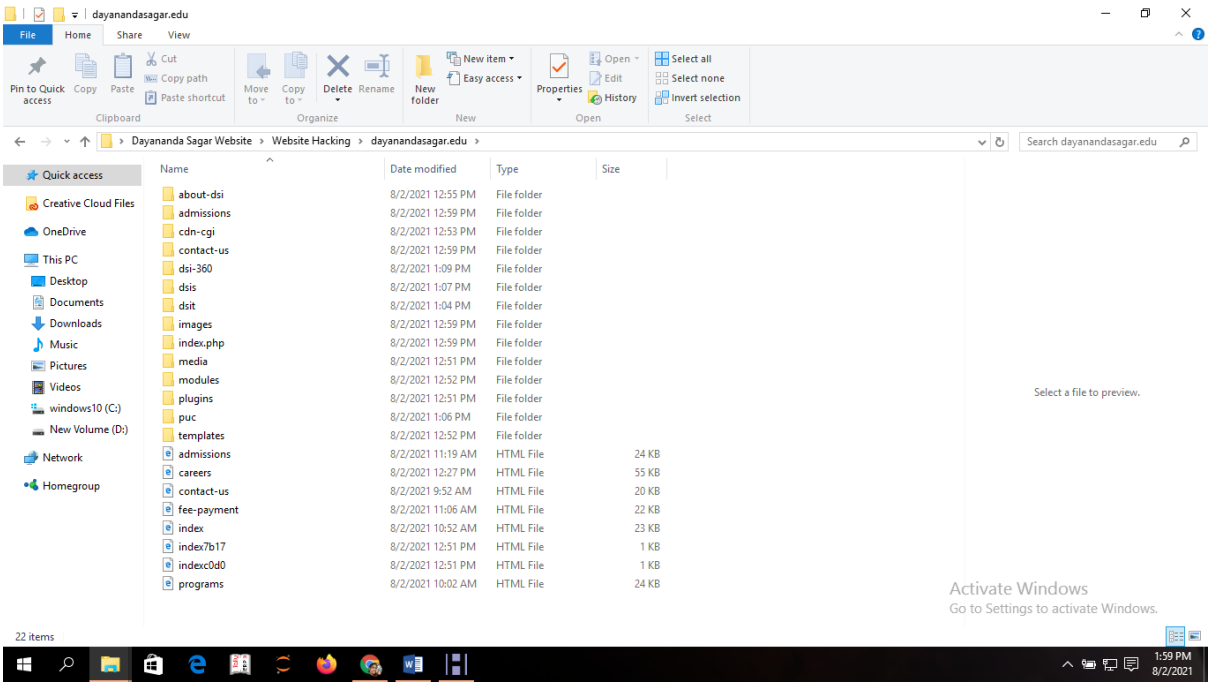
Step 11: The detail information about the URL will be fetched and saved in the folder "Dayananda Sagar Website". U can now open the folder where you can see the the project name given as Website hacking as shown in Step 3.



Step 12: Click on Website hacking file, then the URL address dayanandasagar.edu given in the Step 8 will be visible.

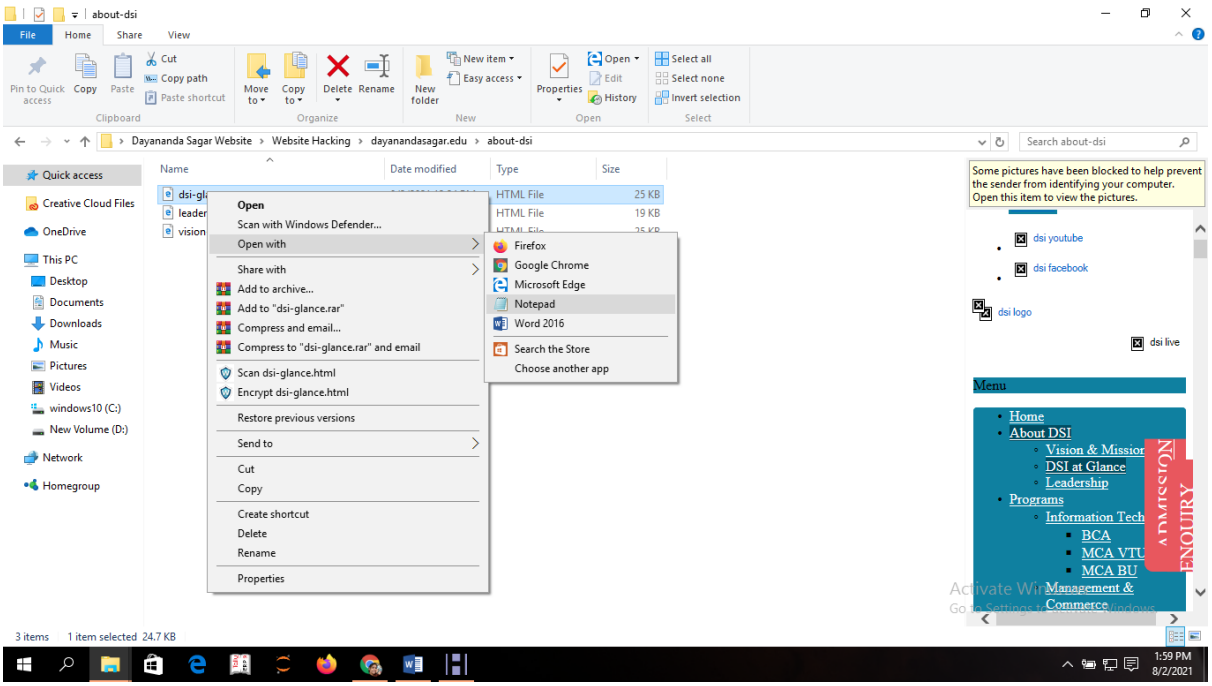


Step 13: Click on the file, dayanandasagar.edu. Now you can find all the files of the original page of the Website will be displayed.

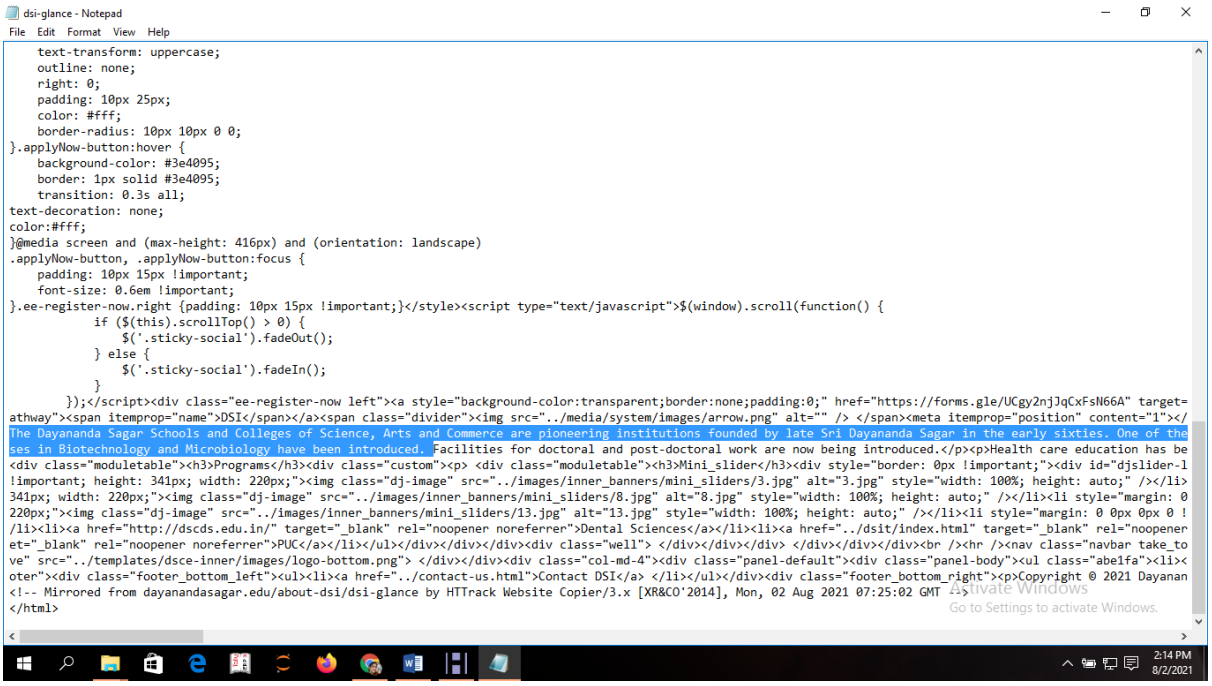


Step 14: Click on any file to alter the content : open with notepad.

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.



Step 15: Contents of the pages is displayed. Now you can alter the Contents.



RESULT:

The main aim is to downloading a website using website copier tool (HTTtack) is completed successfully

EXPT.NO 6(B)	TEXT STEGNOGRAPHY : HIDING THE INFORMATION IN THE TEXT FILE USING SNOW TOOL	DATE:

AIM:

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

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.**

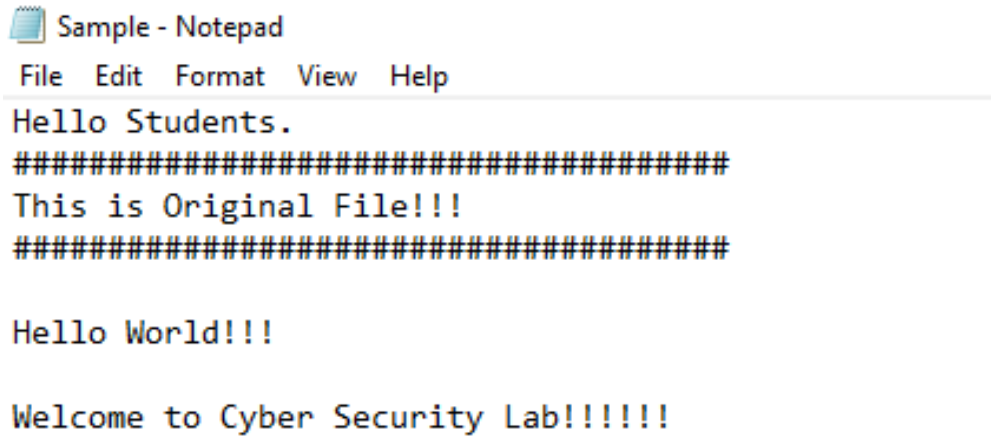


Figure: Text File

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

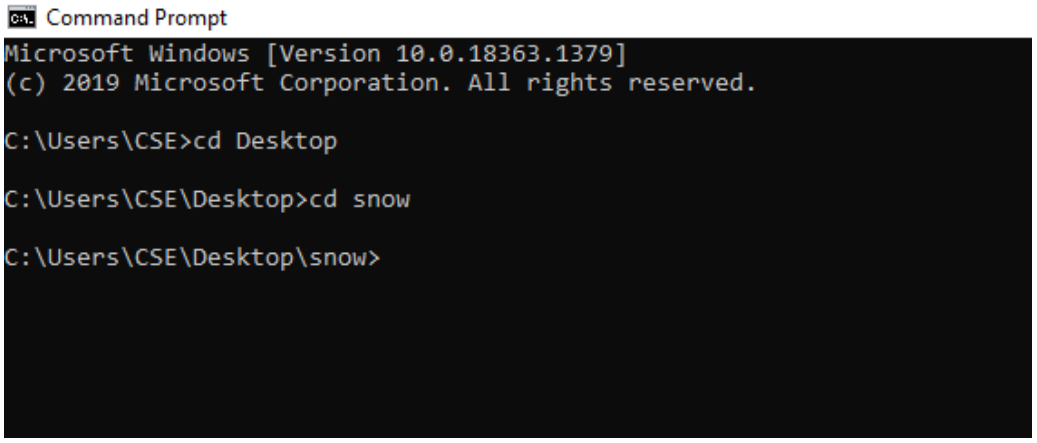


Figure: Changing the Directory

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.

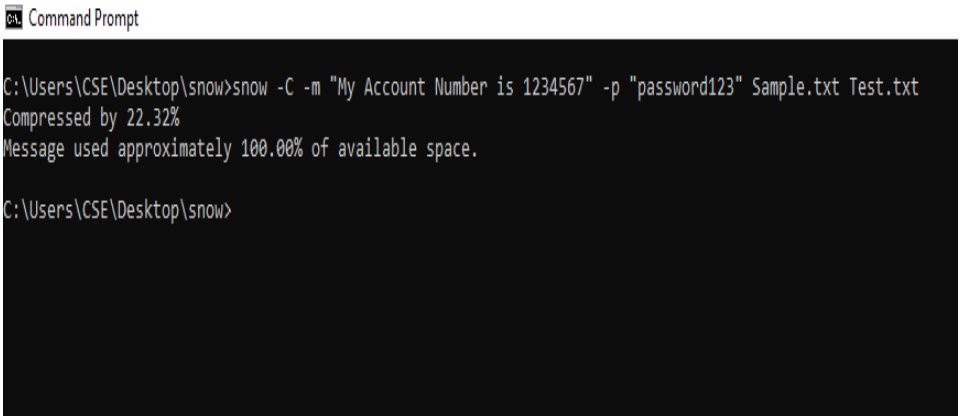


Figure: **White Space Steganography using Snow Tool**

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

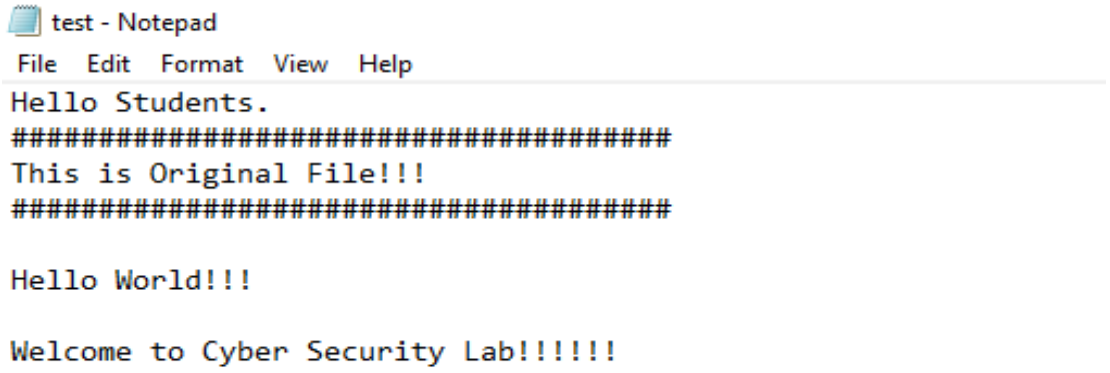


Figure: File Containing Hidden Encrypted Information

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

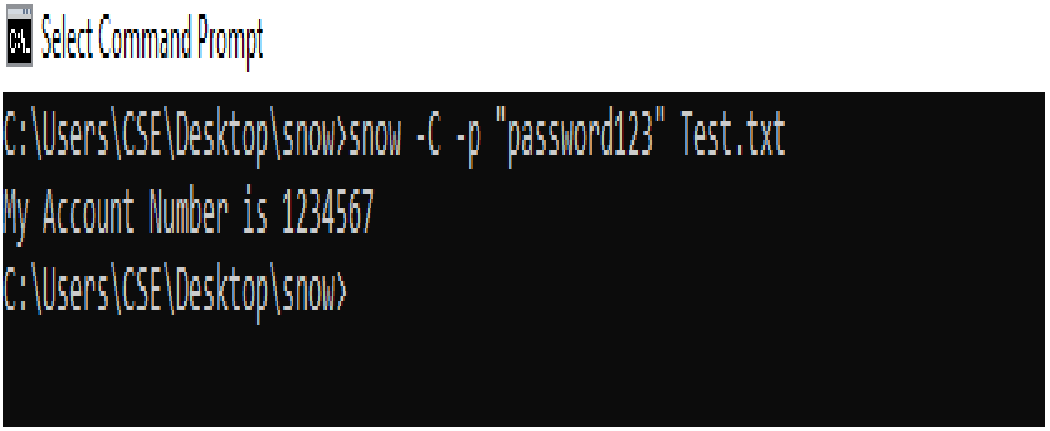


Figure: Decrypting File

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 Stegnography is completed successfully.

EXPT.NO 7(A)	ANALYZE THE PACKET CAPTURE USING WIRESHARK TOOL(TCP)	DATE:

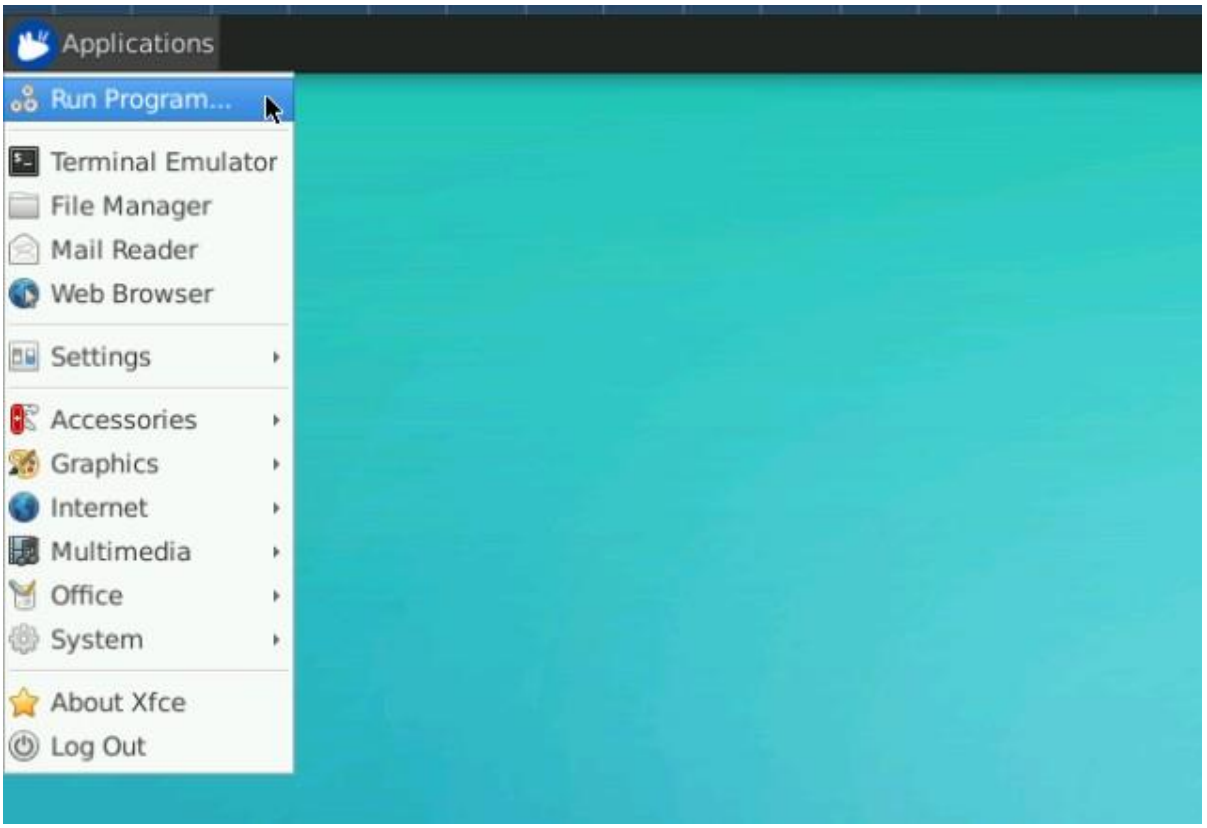
AIM:

Analyze the TCP packet capture using Wireshark tool.

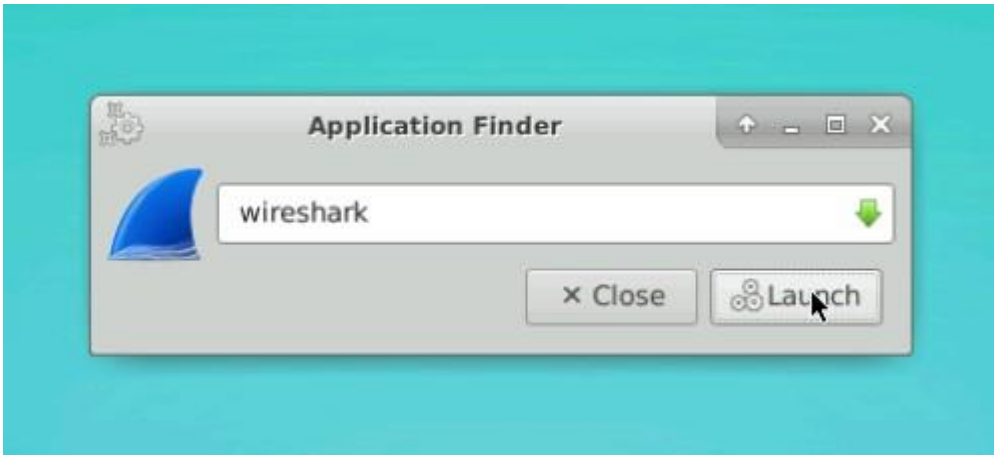
1. Step-1: Capture the real time network traffic using Wireshark

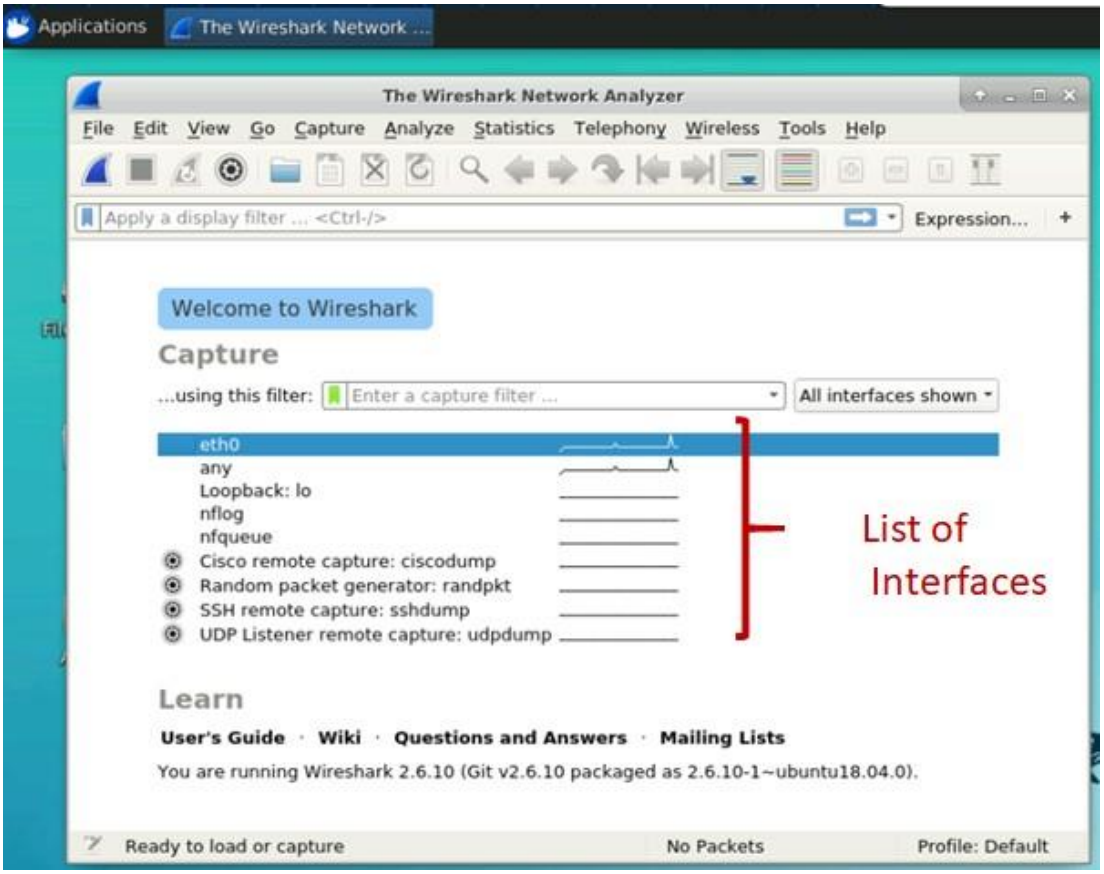
a. Open Wireshark Application

To open the Wireshark go to the Top left corner, click on the icon to open the list ofthe tools available.



Then type Wireshark in the search bar and click on the launch button.

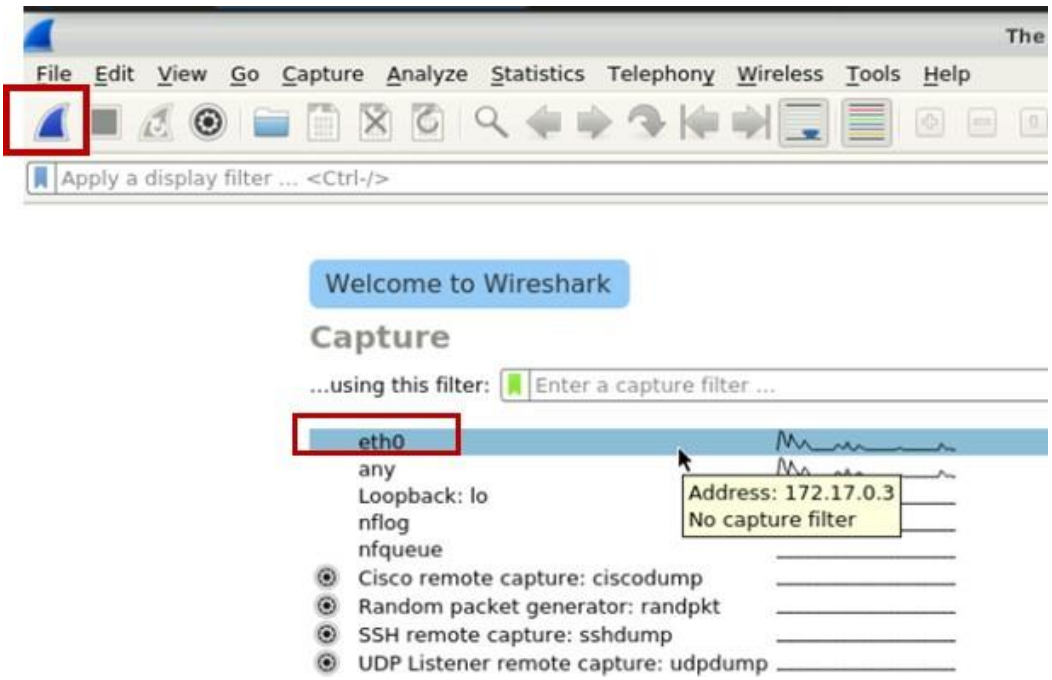




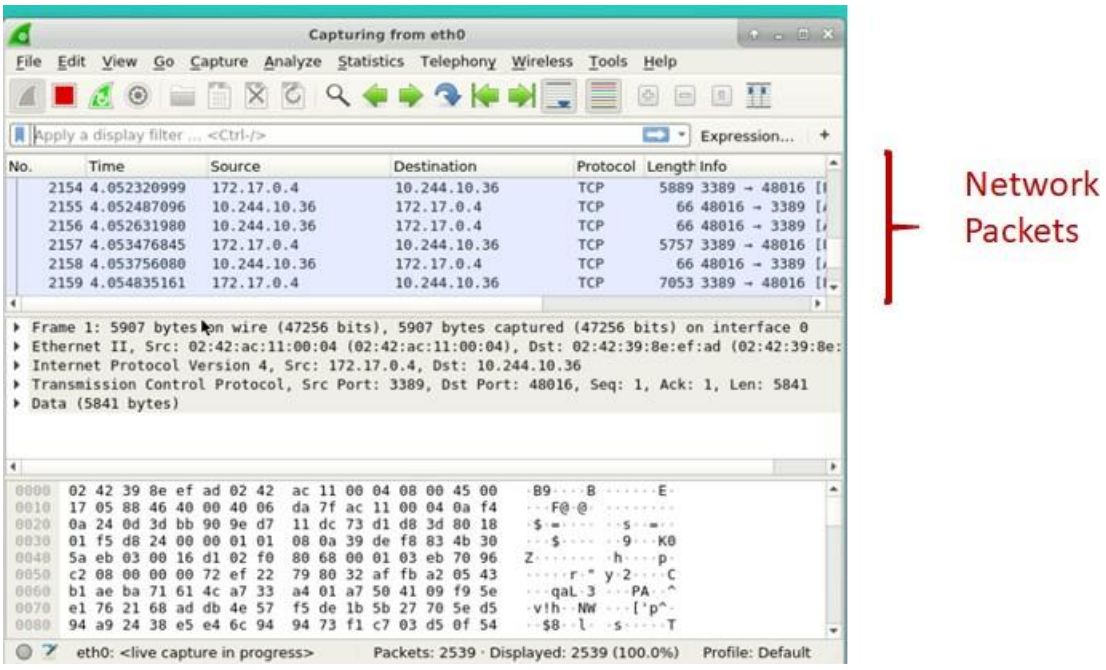
b. Select the network interface

Select eth0 **interface to start capturing the data and Click on this**  **option to**

capture the N packets. This screen is shown below.



Once you click on the capture button, packet capturing will start. The packet capturing screen is shown below.



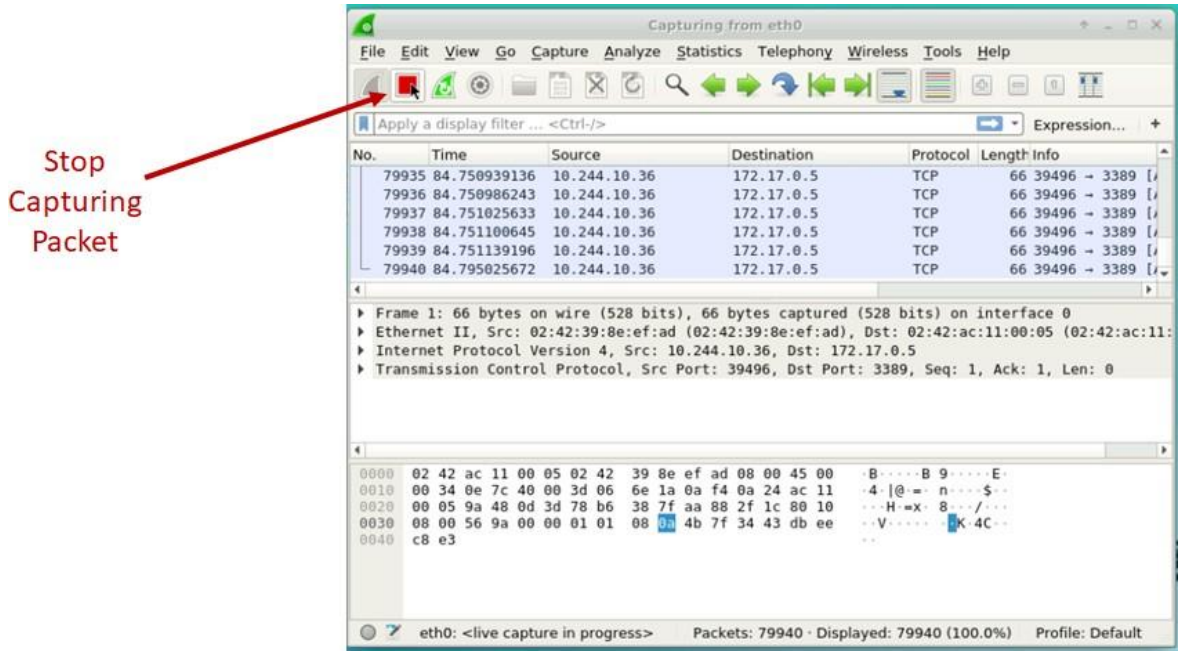
c. Browse a Website

To open the Browser go to the Top left corner, click on the "Application" icon toopen the list of the tools available and select the web browser.

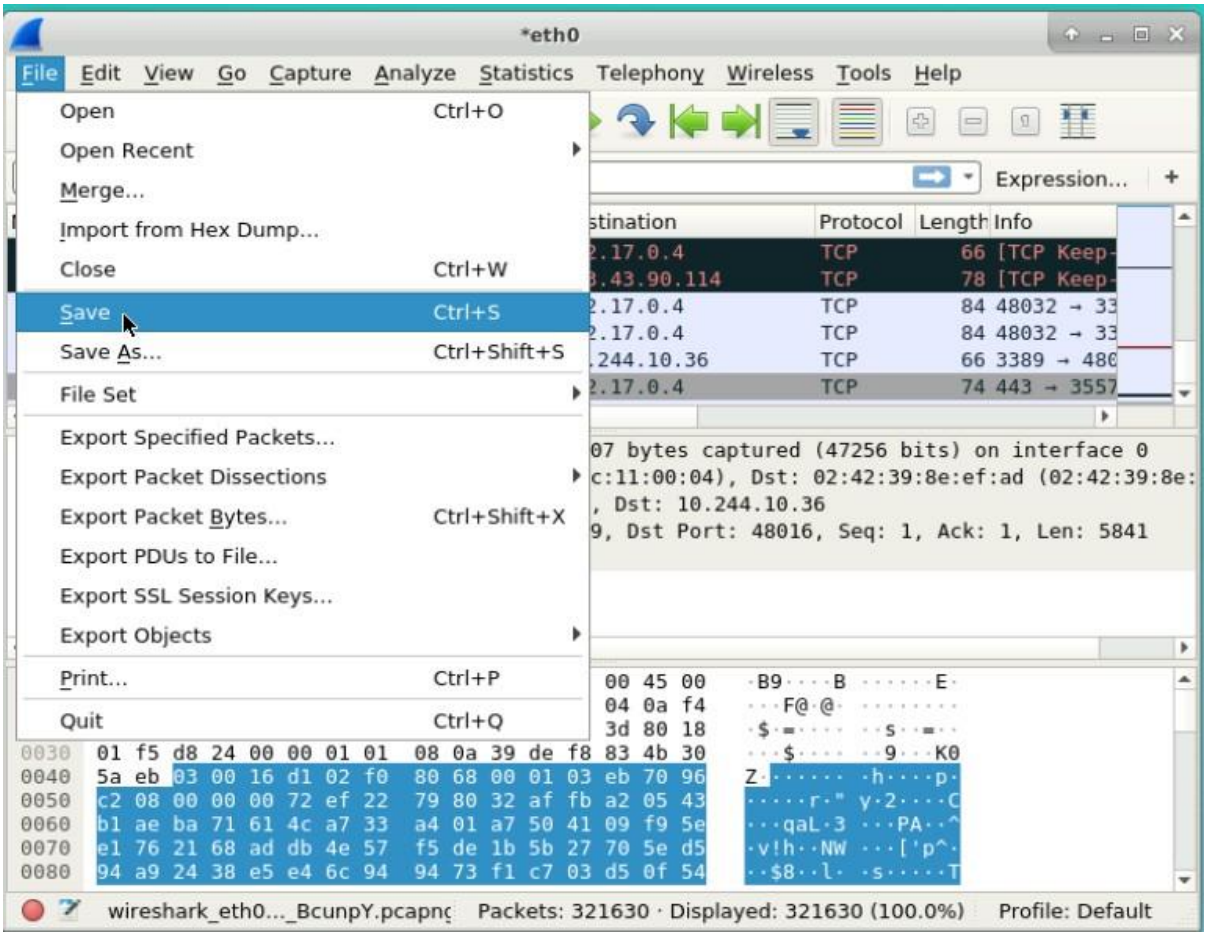
Browse any website in the web browser. For instance www.cdac.in.

d. Save Network Traffic

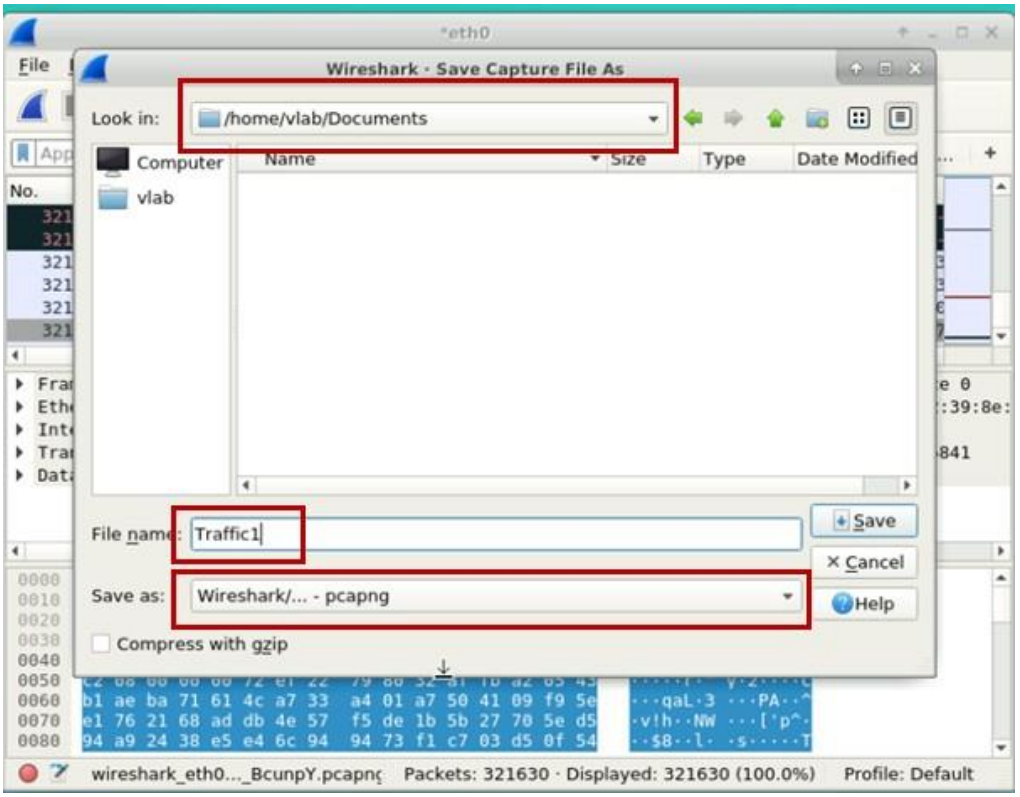
Before saving Network traffic, stop the Wireshark packet capturing by selecting the symbol



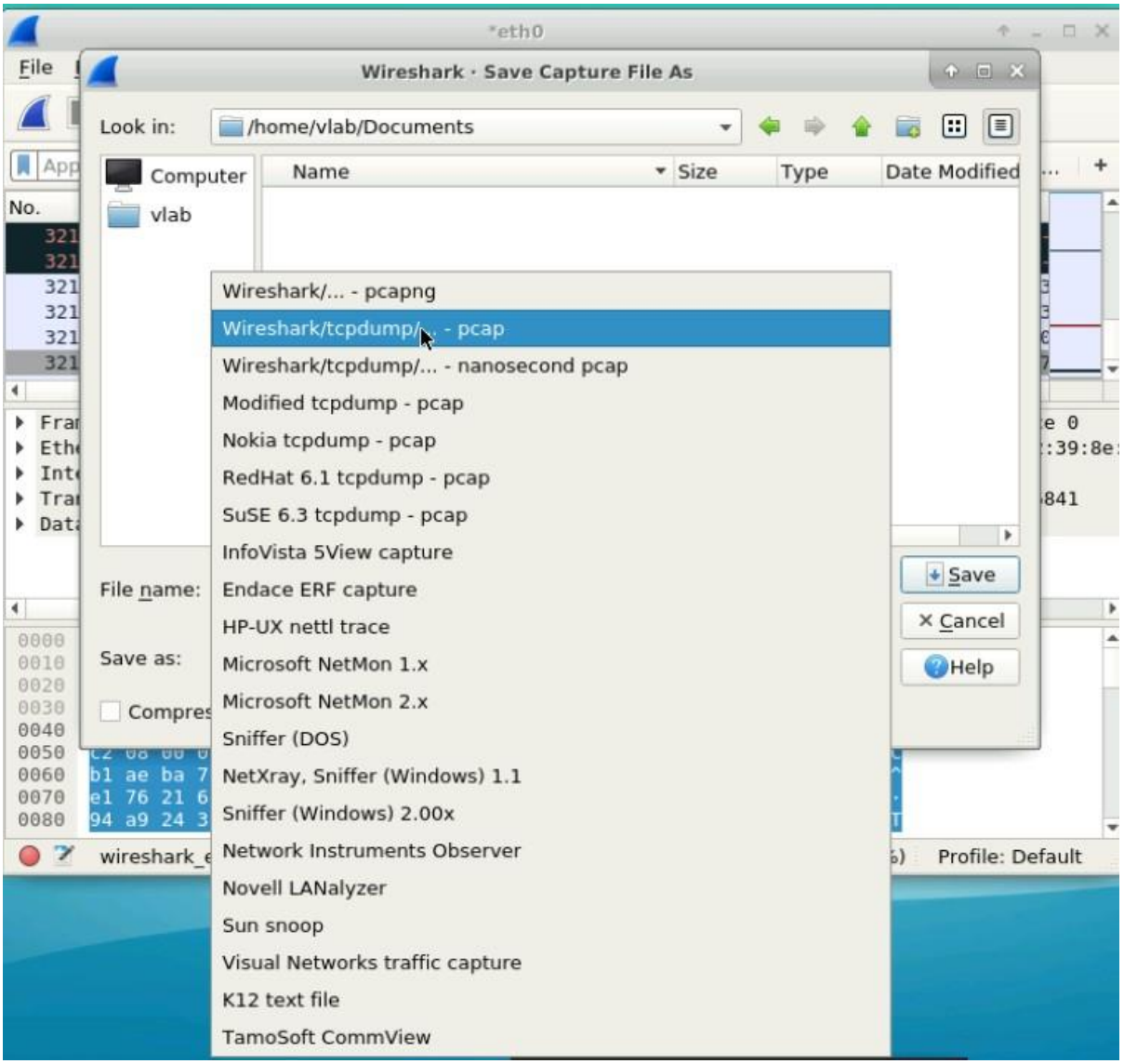
In order to save the captured network packets, go to the top left corner and click on"File" followed by "save" .



Give any name to your file . Here we have given Traffic1 which is shown below:



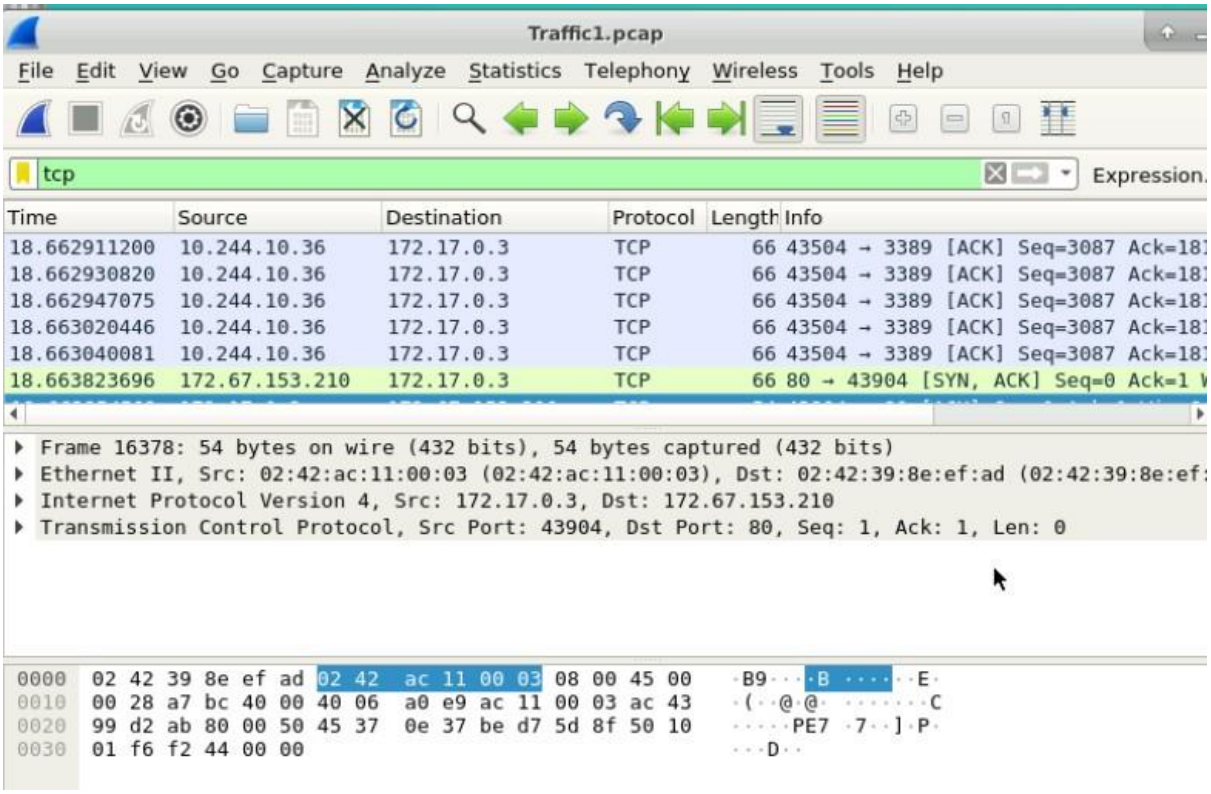
Now select the extension as pcap by clicking on the drop down beside the "save as".Choose the "wireshark/tcpdump- pcap" option and click on the "save" button.



2. Step-2: Following TCP Stream

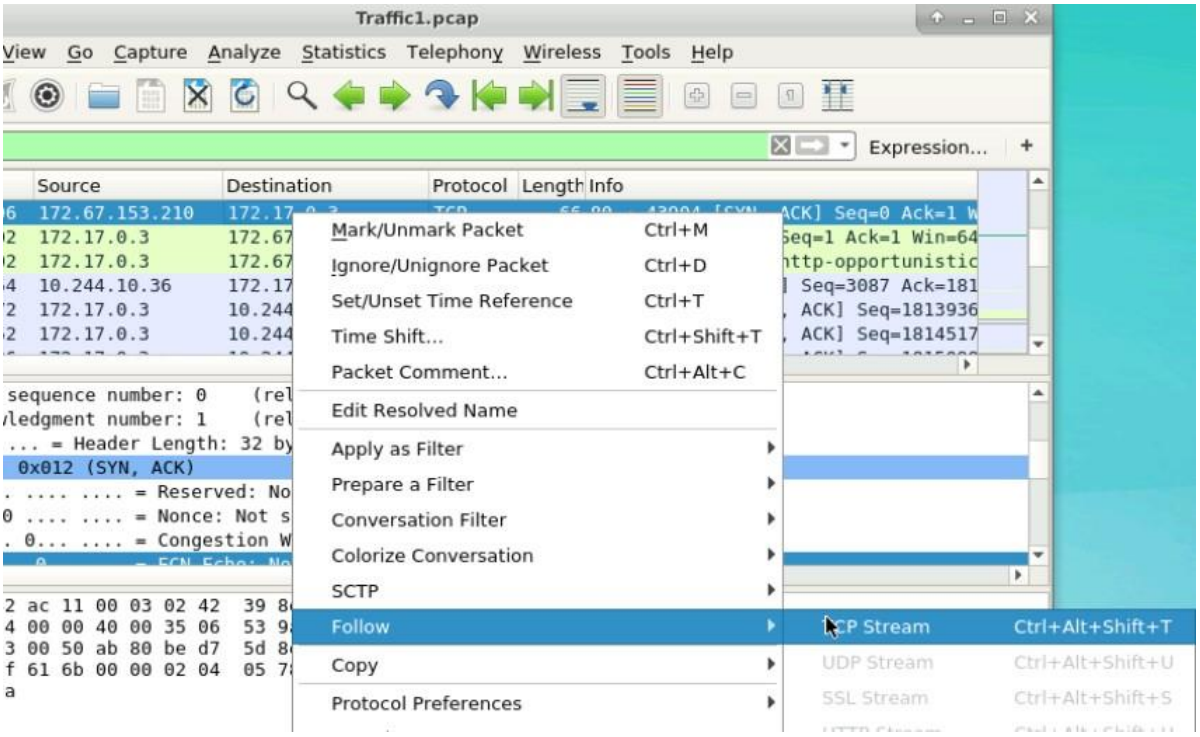
a. Filter tcp traffic

Analyse the TCP packets using the Filter box. Type “tcp” in the Filter box to get allthe TCP packets.



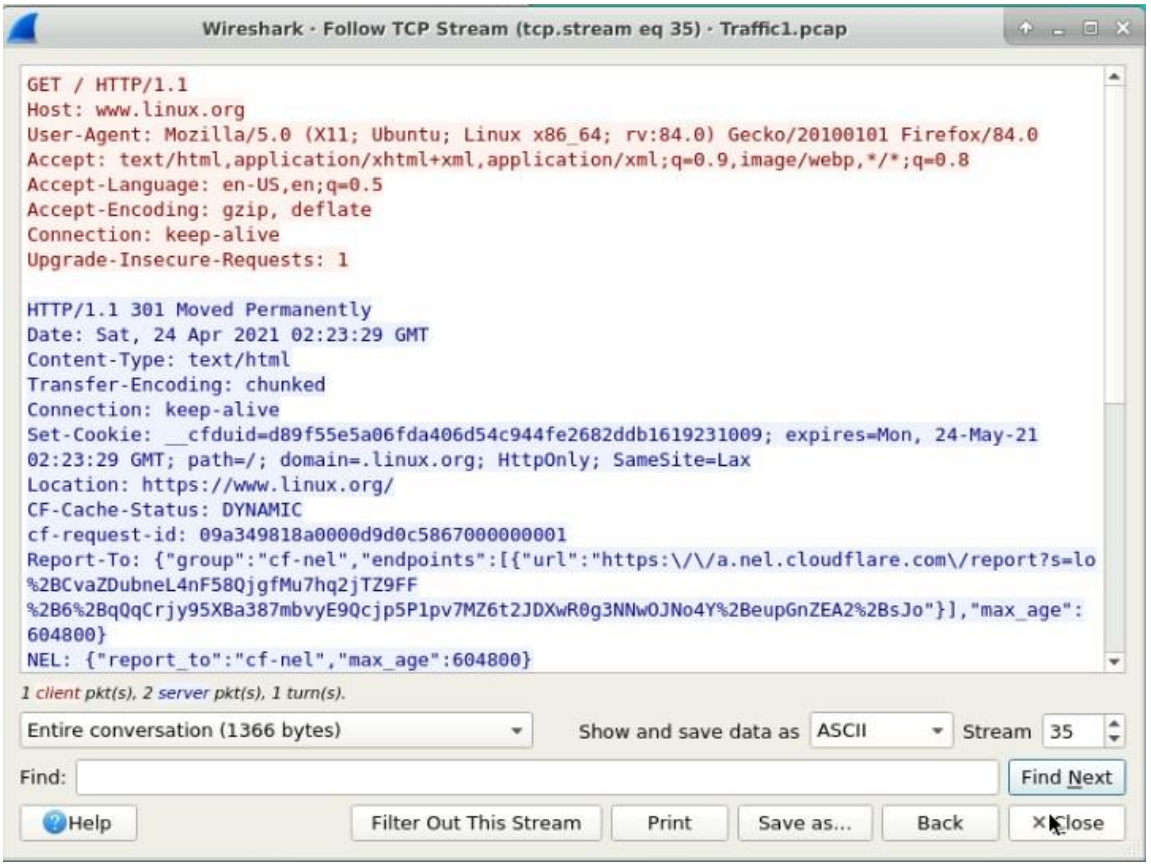
b. Follow TCP Stream

To view the one complete three way tcp handshake connection, right click on anygreen color traffic and select "Follow". Choose "TCP Stream" as given

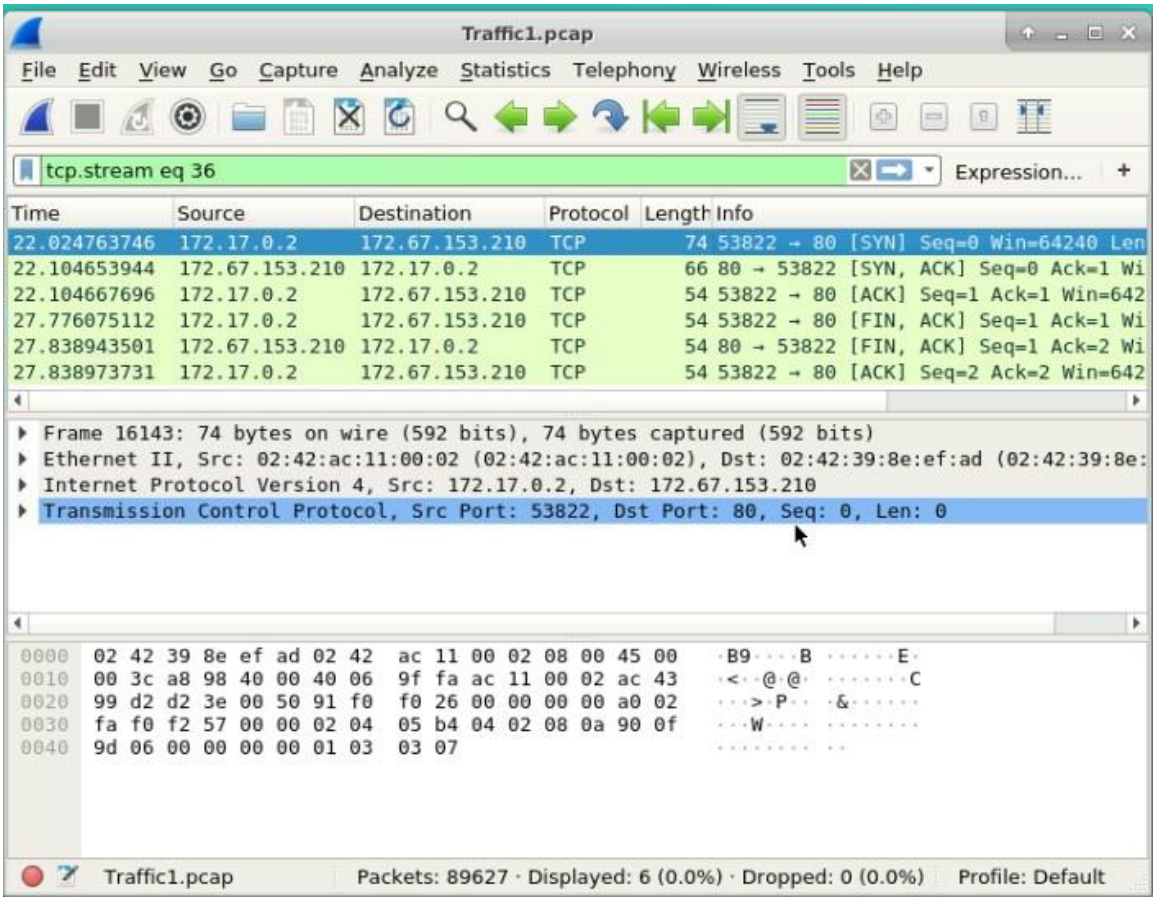


below:

one window will open. Click on the close button.



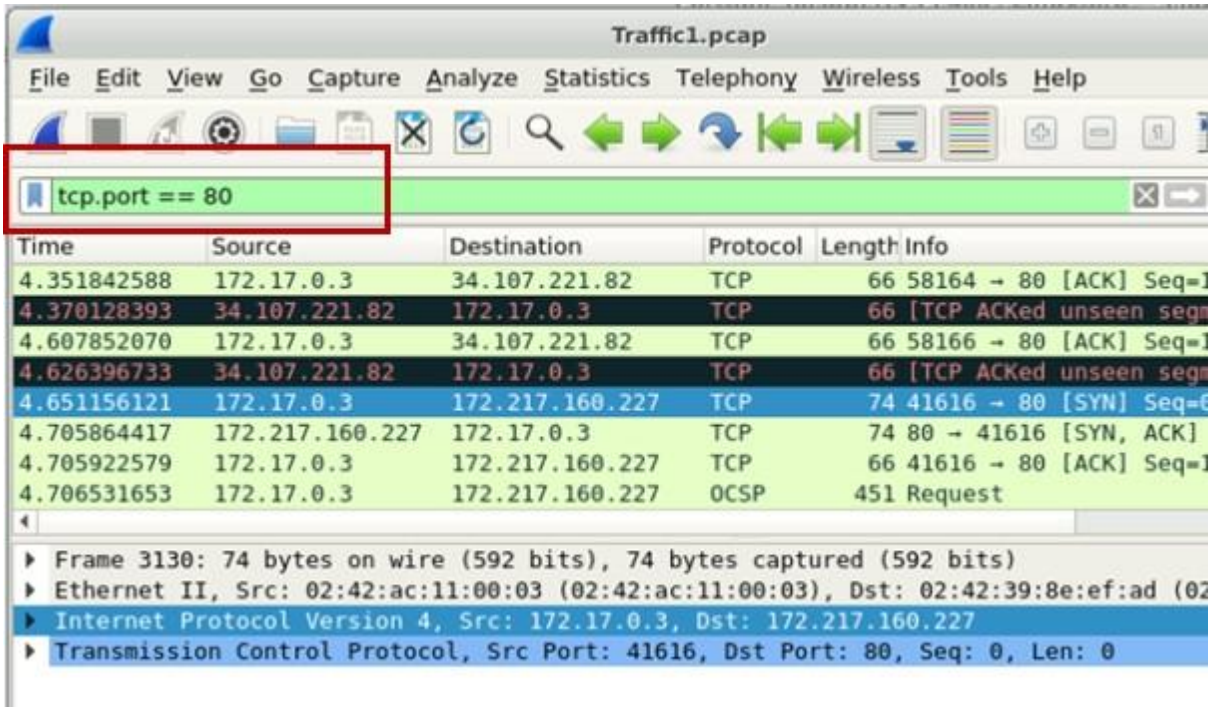
Result after using TCP stream is given below:



3. Step 3: Analyze TCP Header

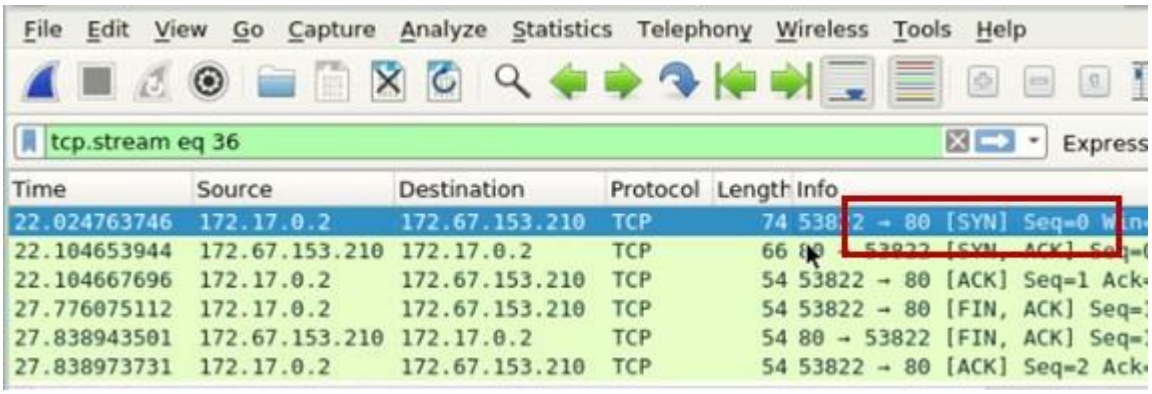
a. Analyze TCP SYN Traffic

Try to observe the TCP SYN traffic captured in the Wireshark packet list pane. Type tcp.port == 80 in the Filter box and press Enter.



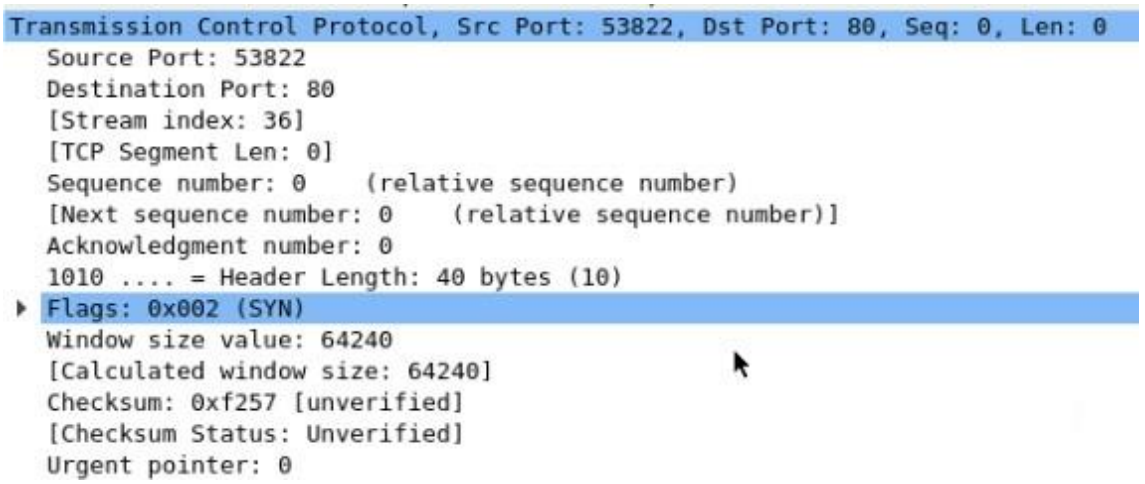
Right click on the first SYN packet and select Follow and then click on TCP Stream.

Click on the Close button. The below screen will be visible.

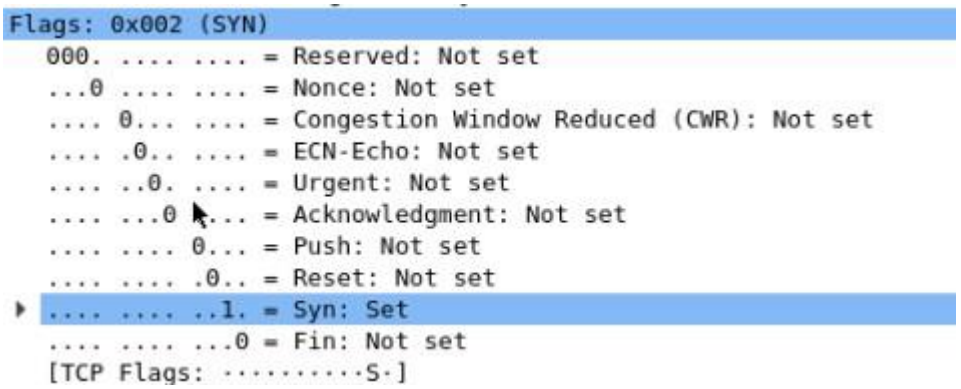


Expand Transmission Control Protocol to view the further details and observe the following:

- Observe the Source port. Notice that it is a dynamic port selected for this connection.
- Observe the Destination port. Notice that it should be 80.
- Observe the Sequence number. Notice that it is 0 (relative sequence number). To see the actual sequence number, select the Sequence number to highlight the sequence number in the bottom Wireshark bytes pane.

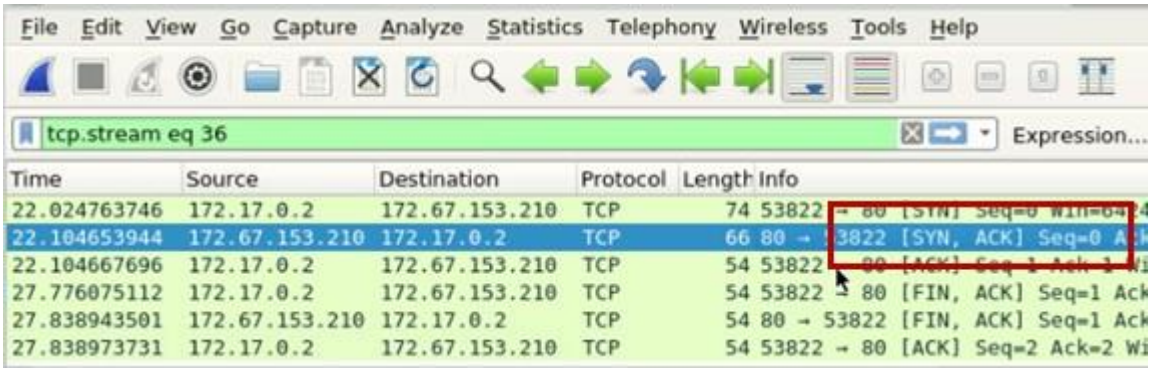


Expand Flags to view flag details. Observe the flag settings. Notice that SYN is set,indicating the first segment in the TCP three-way handshake.



b. Analyze TCP SYN, ACK Traffic

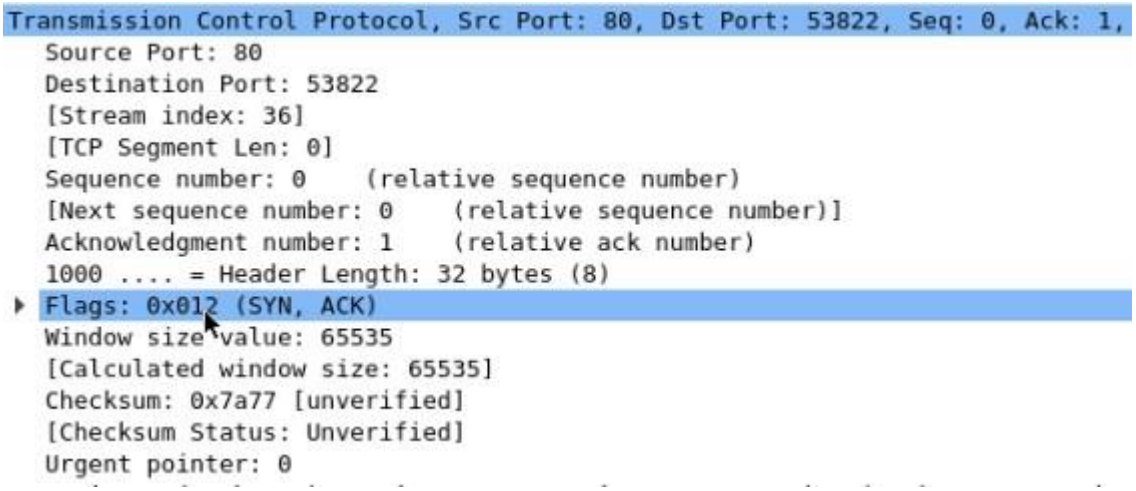
Click on the SYN , ACK **packet and start analyzing TCP SYN, ACK Traffic.**



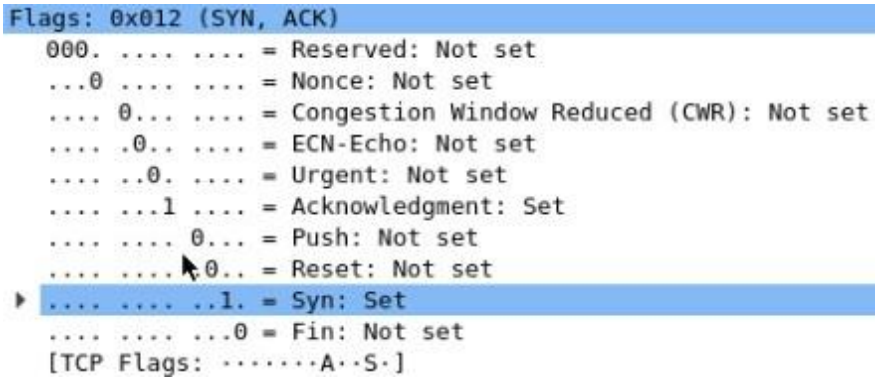
Expand Transmission Control Protocol to view TCP details.

- Observe the Source port. Notice that it will be 80.

- Observe the Destination port. Notice that it is the same dynamic port selected forthis connection.
- Observe the Sequence number. Notice that it is 0 (relative sequence number). To see the actual sequence number, select Sequence number to highlight the sequence number in the bottom Wireshark bytes pane.
- Observe the Acknowledgement number. Notice that it is 1 (relative ack number). To see the actual acknowledgement number, select Acknowledgement number tohighlight the acknowledgement number in the bottom pane. Notice that the actual acknowledgement number is one greater than the sequence number in the previous segment.

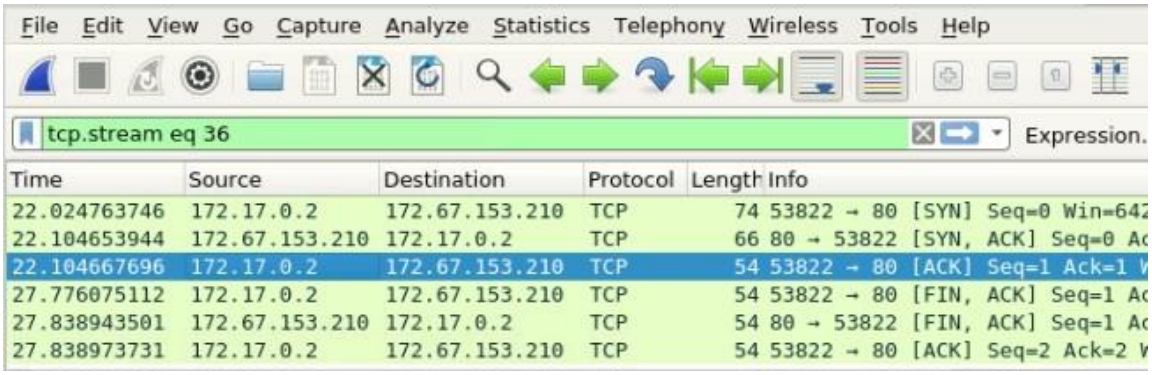


Expand Flags to view flag details. Observe the flag settings. Notice that SYN and ACK areset, indicating the second segment in the TCP three-way handshake.



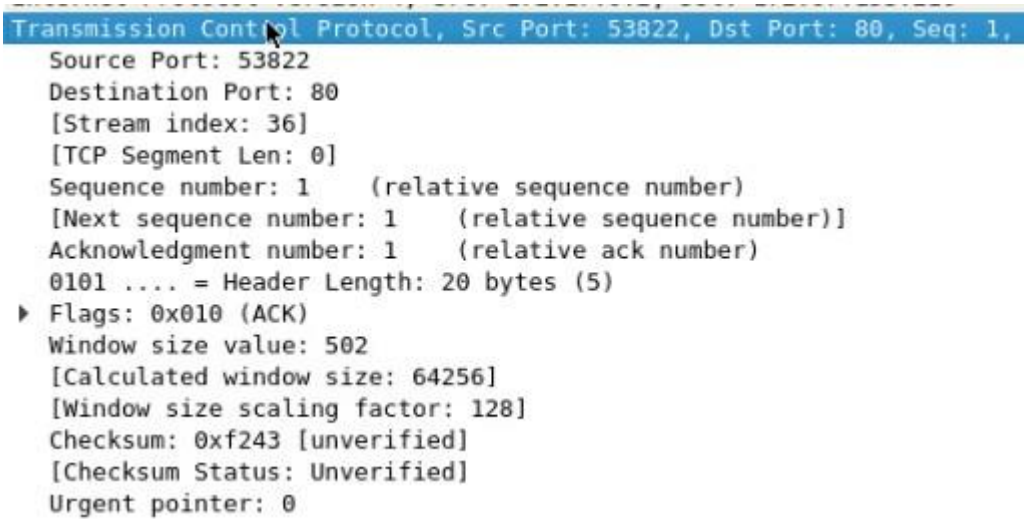
c. Analyze TCP ACK Traffic

Click on the ACK **packet and start analyzing TCP ACK Traffic.**



Expand Transmission Control Protocol to view TCP details.

- Observe the Source port. Notice that it is the same dynamic port selected for this connection.
- Observe the Destination port. Notice that it should be 80.
- Observe the Sequence number. Notice that it is 2 (relative sequence number).
- Observe the Acknowledgement number. Notice that it is 2 (relative ack number).

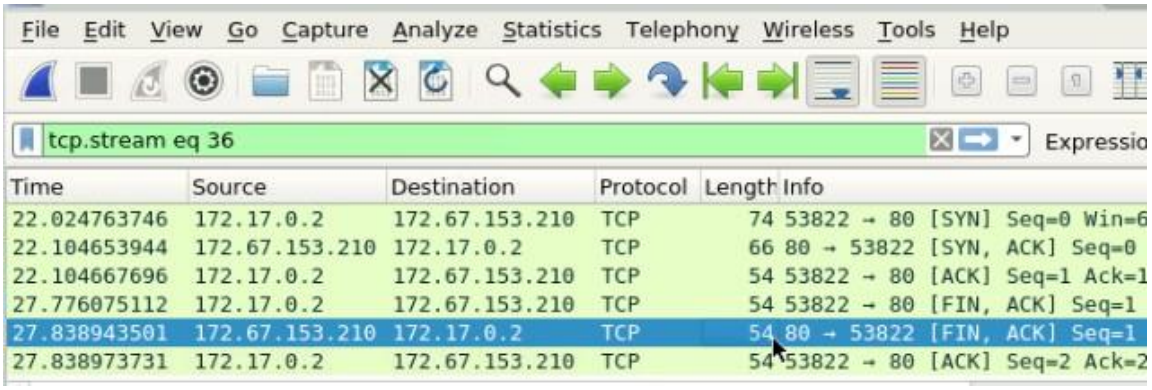


Expand Flags to view flag details. Observe the flag settings. Notice that ACK is set, indicating the third segment in the TCP teardown handshake. The client has acknowledged the server closing the TCP connection.

```
Flags: 0x010 (ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·····A····]
```

d. Analyze TCP FIN ACK Traffic

Click on the FIN, ACK **packet and start analyzing TCP FIN, ACK Traffic.**

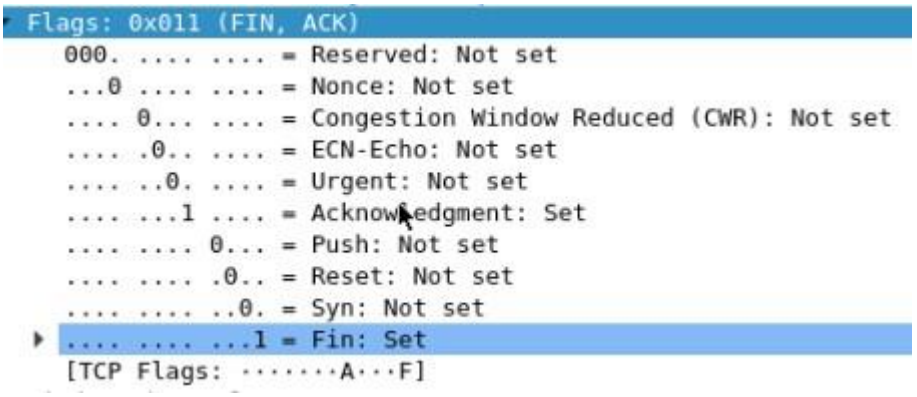


Expand Transmission Control Protocol to view TCP details.

- Observe the Source port. Notice that it should be 80.
- Observe the Destination port. Notice that it is the same dynamic port selected forthis connection.
- Observe the Sequence number. Notice that it is 1 (relative sequence number).
- Observe the Acknowledgement number. Notice that it is 2 (relative ack number).

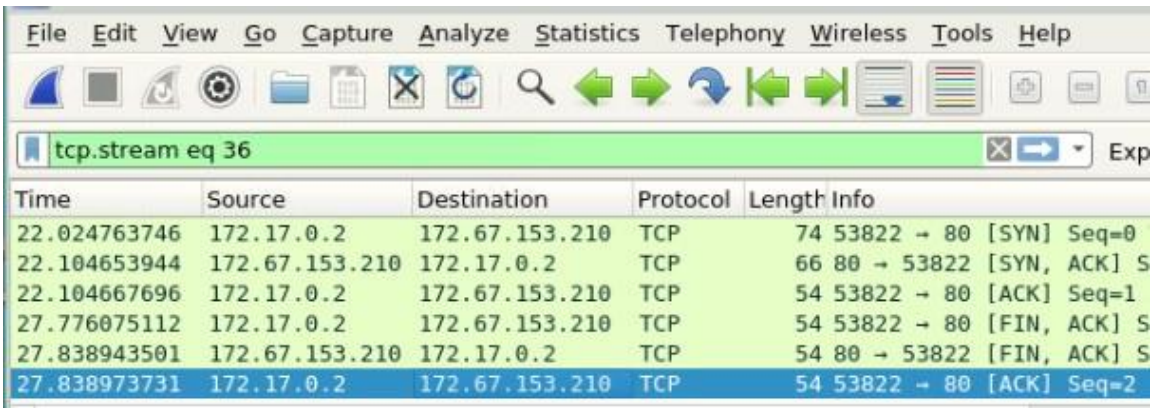
```
Transmission Control Protocol, Src Port: 80, Dst Port: 53822, Seq: 1, Ack: 2, Len: 0
    Source Port: 80
    Destination Port: 53822
    [Stream index: 36]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 2    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x011 (FIN, ACK)
    Window size value: 64
    [Calculated window size: 65536]
    [Window size scaling factor: 1024]
    Checksum: 0xbace [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
```

Expand Flags to view flag details. Observe the flag settings. Notice that FIN and ACK are set, indicating the second segment in the TCP three-way handshake. The server has indicated it is closing the TCP connection with the client.



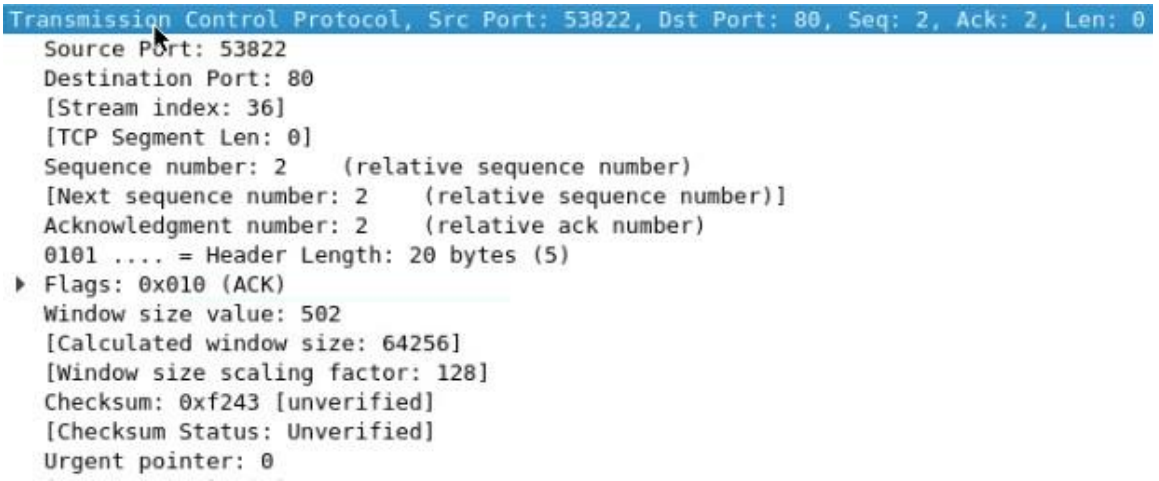
e. Analyze TCP FIN ACK Traffic

Click on the ACK **packet and start analyzing TCP ACK Traffic.**



Expand Transmission Control Protocol to view TCP details.

- Observe the Source port. Notice that it is the same dynamic port selected for this connection.
- Observe the Destination port. Notice that it must be 80.
- Observe the Sequence number. Notice that it is 2 (relative sequence number).
- Observe the Acknowledgement number. Notice that it is 2 (relative ack number).



Expand Flags to view flag details. Observe the flag settings. Notice that ACK is set, indicating the third segment in the TCP teardown handshake. The client has acknowledged the server closing the TCP connection.

EXPT.NO 7(B)	ANALYZE THE PACKET CAPTURE USING WIRESHARK TOOL(FTP)	DATE:

AIM:

The main aim is to analyze the packet capturing using wire shark tool.

PROCEDURE:

Wireshark is a software tool used to monitor the network traffic through a network interface. It is the most widely used network monitoring tool today. Wireshark is loved equally by system administrators, network engineers, network enthusiasts, network security professionals and black hat hackers.

The basic features of Wireshark are:

Packet Monitor: This segment visually shows the packets flowing inside the network. There are color codes for each type of packet. The packets are shown with the following information :

1. Source address
2. Destination address
3. Packet type
4. Hex dump of the packet
5. Contents of the packet in text
6. Source port(if applicable)
7. Destination port(if applicable)

Import from a capture file: This feature lets you import packets dump from a capture file to analyse further. There are many formats supported by Wireshark, some of them are:

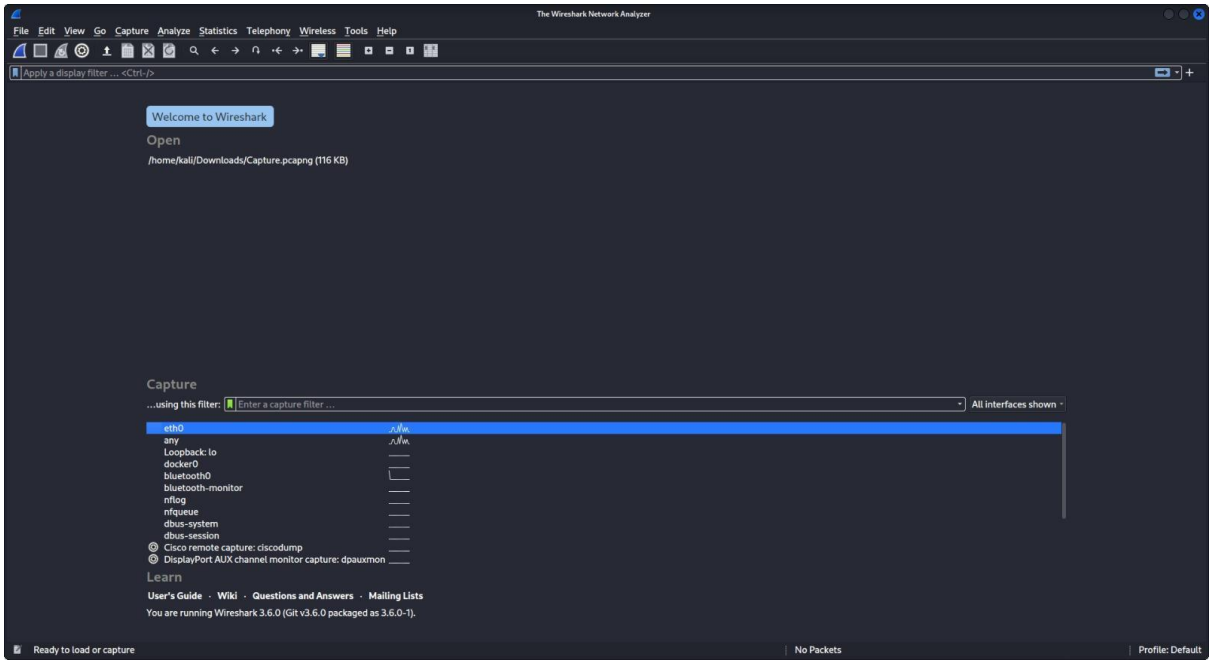
- **pcapng**
- **libpcap**
- **Oracle snoop and atmsnoop**

Export to a capture file: Wireshark lets you save the results as a capture file to continue working on them at later point of time.

STEPS

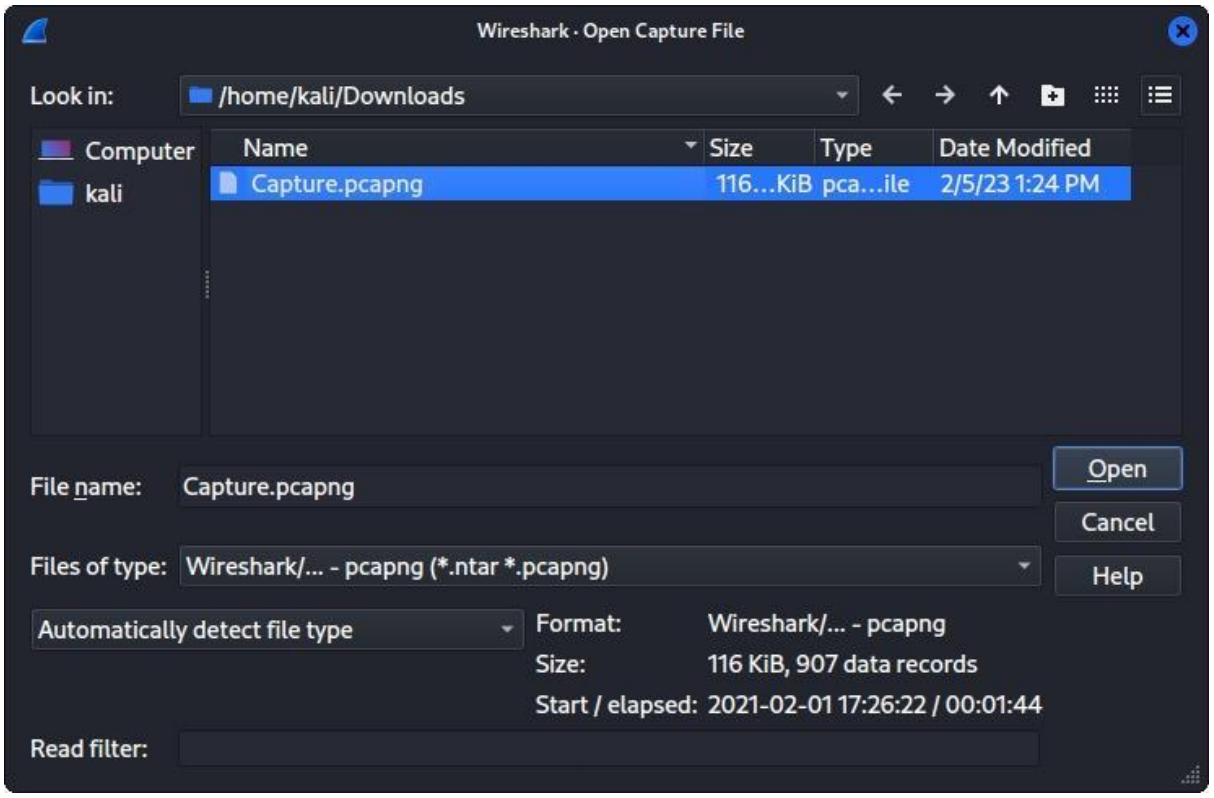
Step 1: Start the VM and launch kali Linux.

Step 2: Search for Wireshark tool in kali Linux by clicking on the top left corner and open the Wireshark tool.

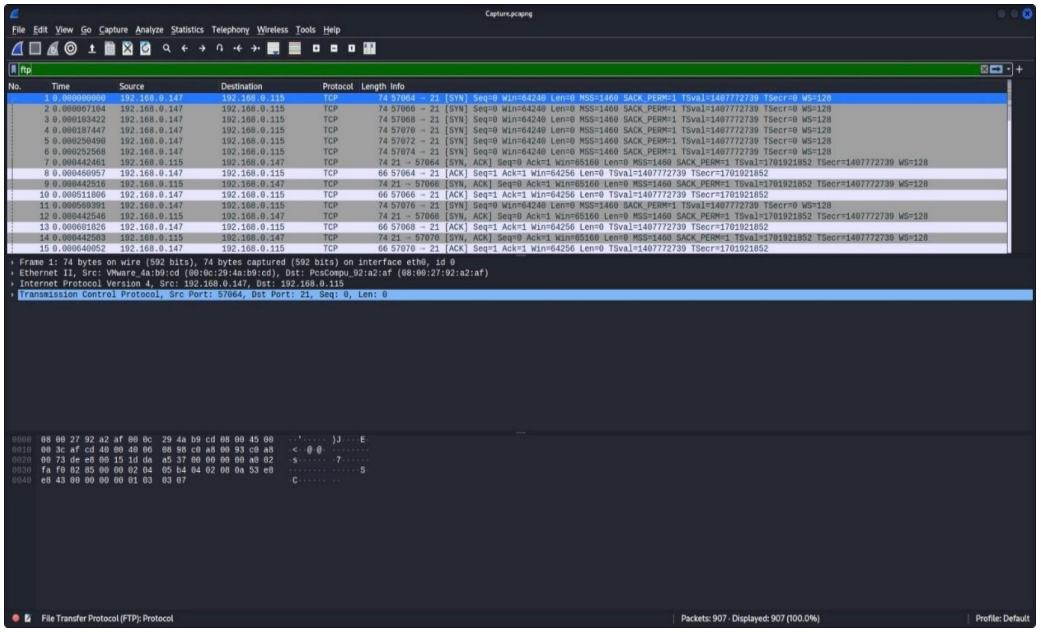


Step 3: After the Wireshark interface is open, navigate to the files menu in the upper left corner.

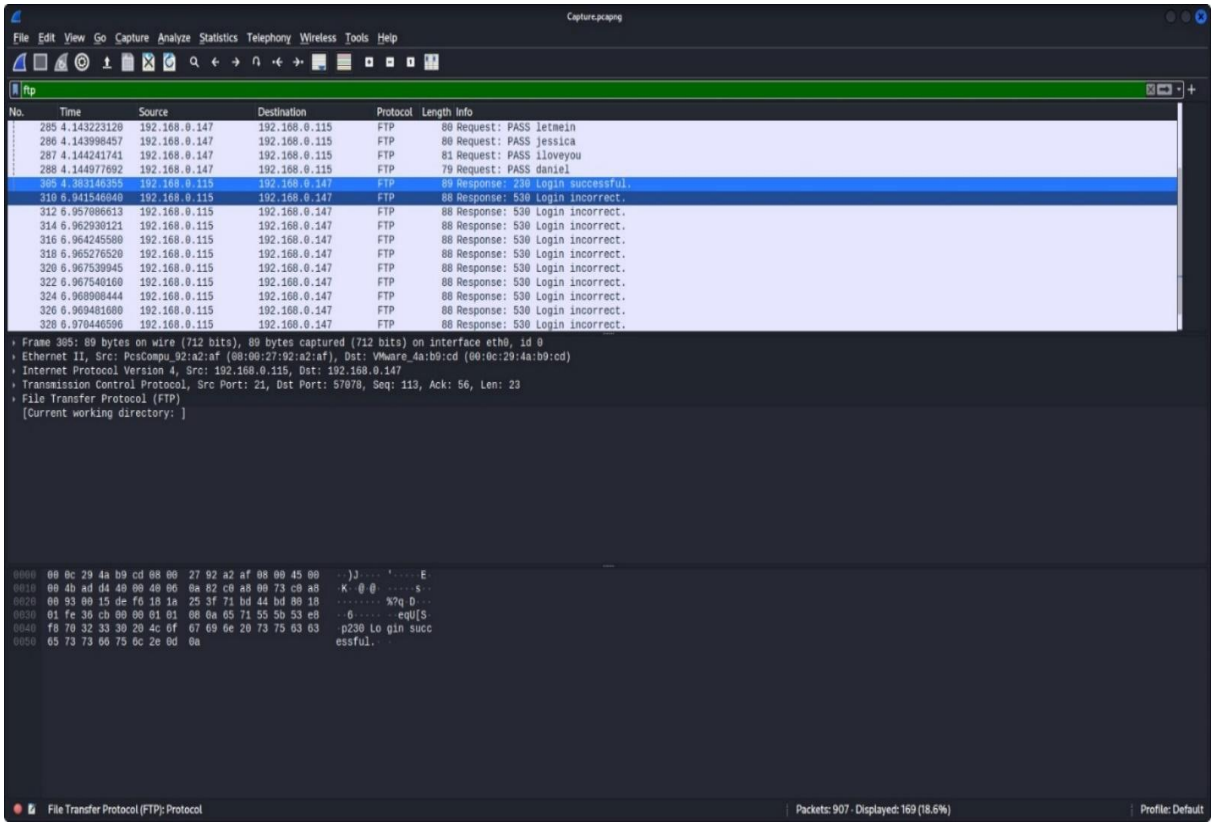
Step 4: Click on the captured file to open it. This file already exists in the system.(.pcapng file)



Step 5: We are attempting to evaluate the packets transmitted over the FTP protocol. Filter the ftp packets by entering 'ftp' into the filter box and press enter.

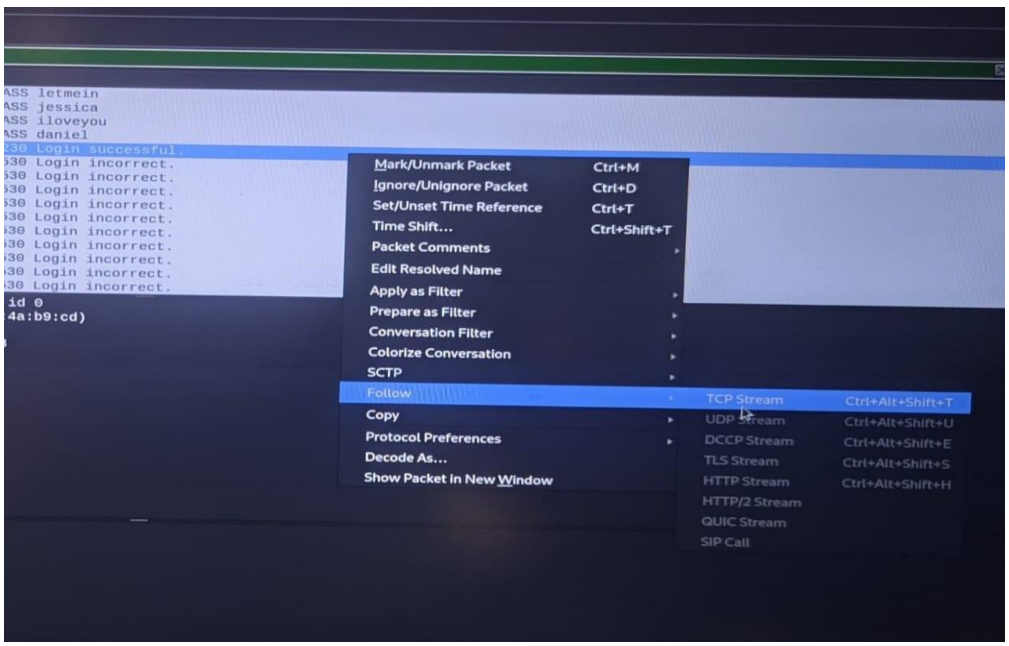


Step 6: You can now observe the packets being transmitted using the ftp protocol. More requests and replies may be found as you scroll below.

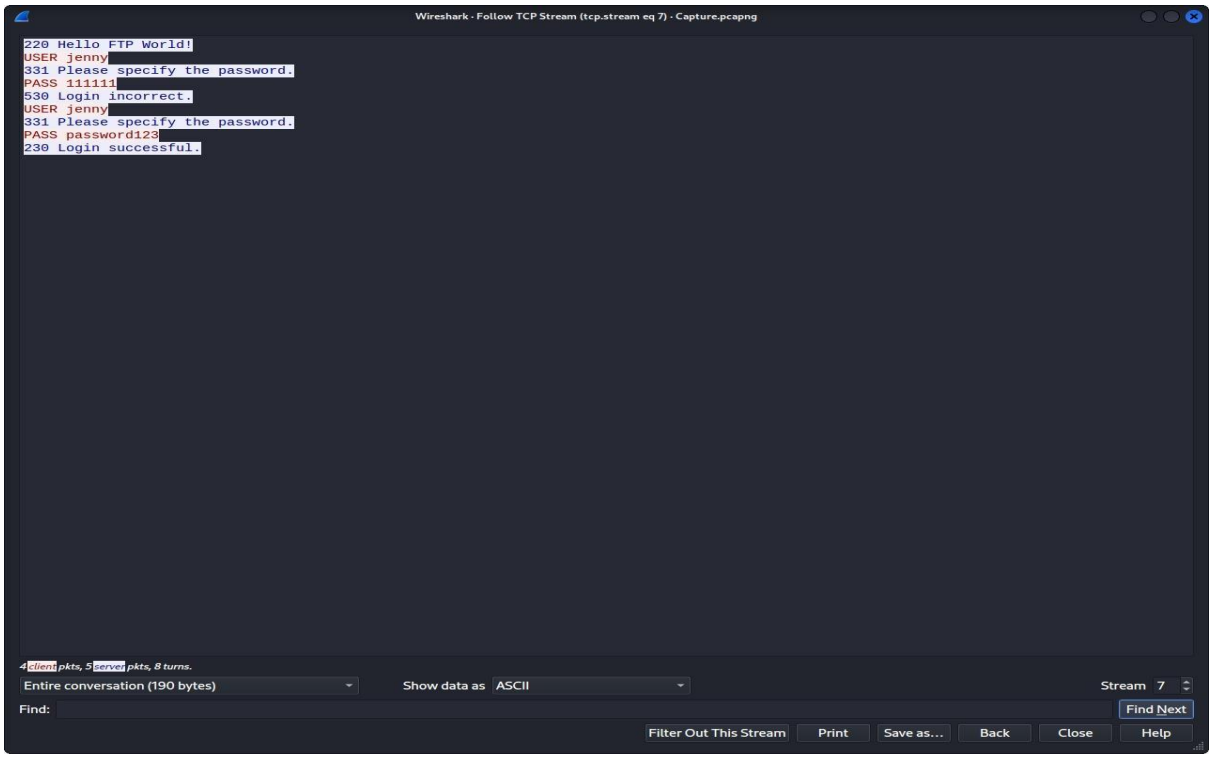


Step 8: You can notice a 'login successful' packet when you scroll down to examine.

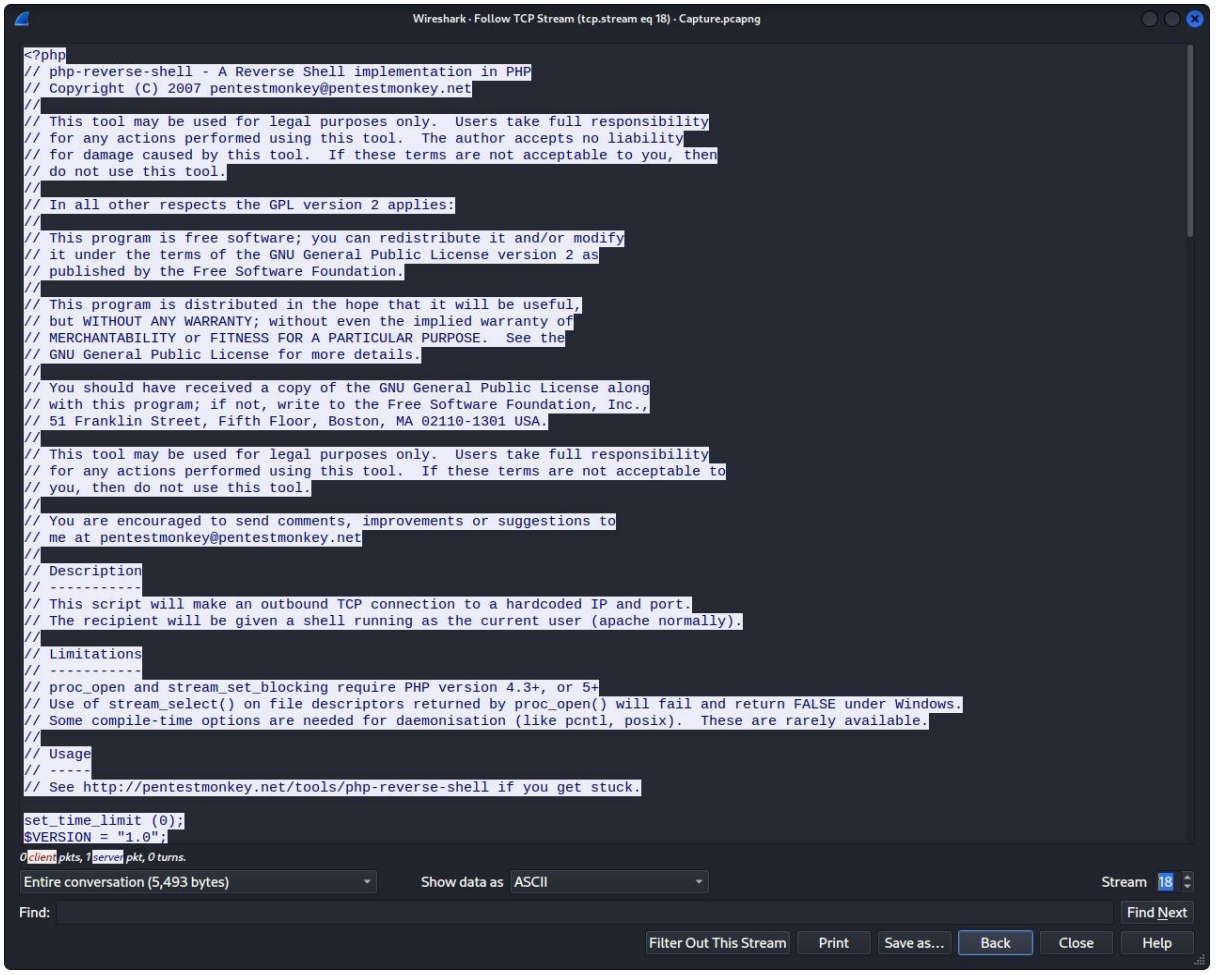
Step 9: Right-click on the packet, select Follow □TCP stream



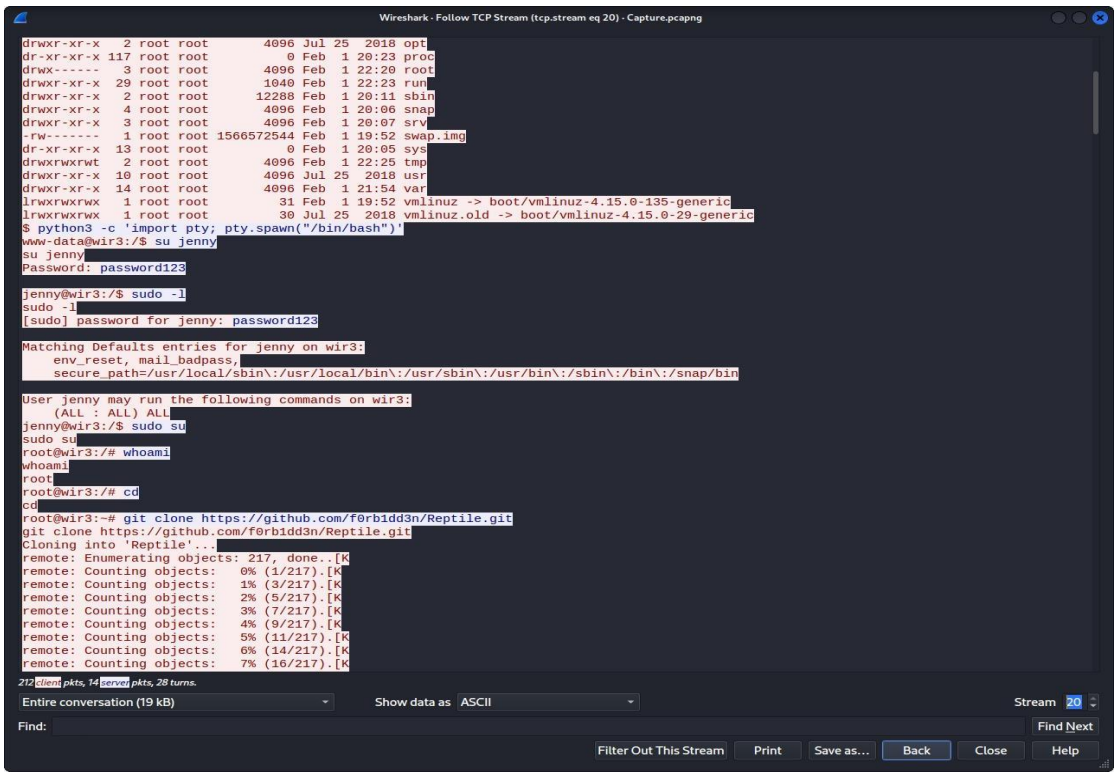
Step 10: Now try to analyze the packet by changing the streams in the bottom left corner.



Step 11: In stream 16, we can see the attacker trying to gain the “Initial Access”. The attacker has installed a shell.php file in the var/www/html.



Step 12: In stream 18,The reverse shell.php enables the attacker to track all of the user's online behavior.



Step 13: In stream 20, we can see the attacker is trying to gain access to the complete console by trying to login to ssh using the same password. This is called the ‘Privilege Escalation’.

Step 14: In stream 20, We learn that the intruder set up a backdoor so he can enter the system whenever he wants. This is called ‘Persistence’

Summary:

RESULT:

The main aim is to analyze the packet capture using wire shark tool is completed successfully.

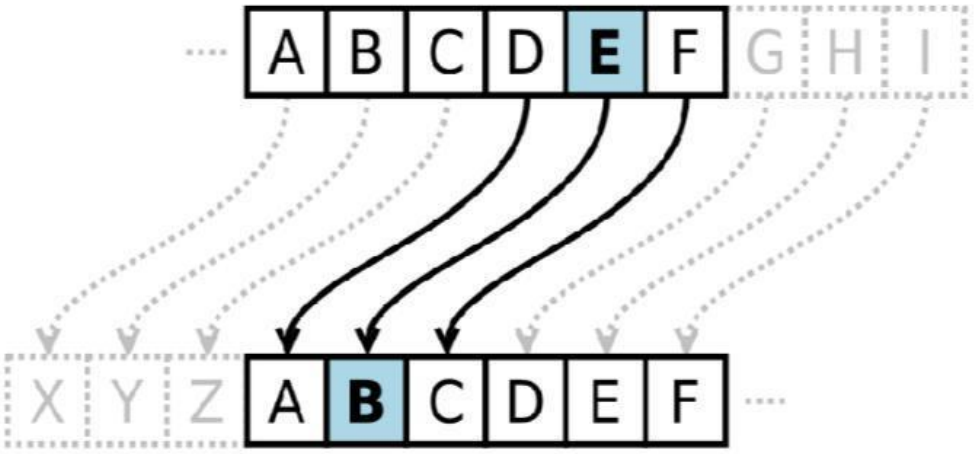
EXPT.NO 8(A)	IMPLEMENTATION OF CAESAR CIPHER USING C PROGRAM	DATE:

AIM:

To implement the simple substitution technique named Caesar cipher using C language..

PROCEDURE:

DESCRIPTION: To encrypt a message with a Caesar cipher, each letter in the message is changed using a simple rule: shift by three. Each letter is replaced by the letter three letters ahead in the alphabet. A becomes D, B becomes E, and so on. For the last letters, we can think of alphabet as a circle and "wrap around". W becomes Z, X becomes A, Y becomes B, and Z becomes C. To change a message back, each letter is replaced by the one three before it.



ALGORITHM:

STEP-1: Read the plain text from the user.

STEP-2: Read the key value from the user.

STEP-3: If the key is positive then encrypt the text by adding the key with each character in the plain text.

STEP-4: Else subtract the key from the plain text.

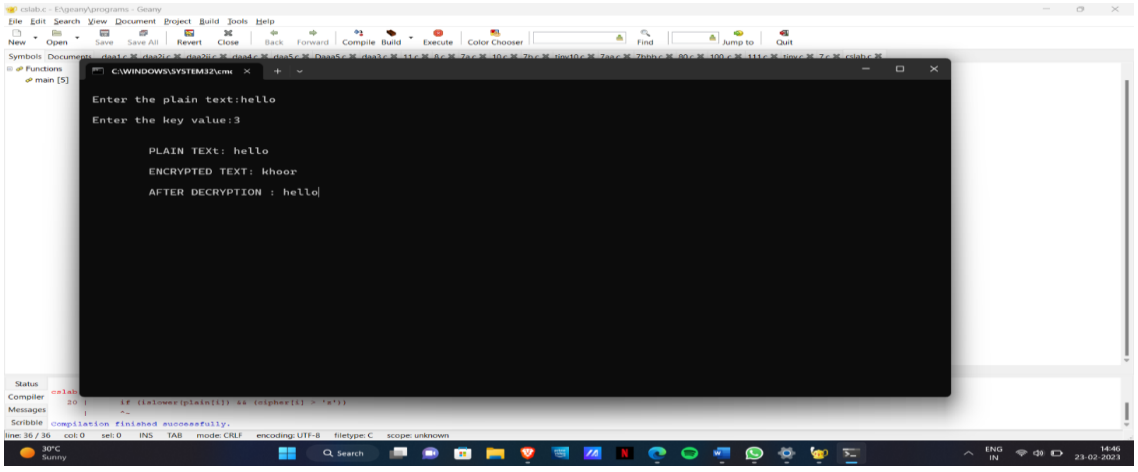
STEP-5: Display the cipher text obtained above.

PROGRAM: (Caesar Cipher)

```
#include <stdio.h>
#include <string.h>
#include<conio.h>
#include <ctype.h>
int main()
{
char plain[10], cipher[10];
int key,i,length;
                                printf("\n Enter the plain text:");
                                scanf("%s", plain);
                                printf("\n Enter the key value:");
                                scanf("%d", &key);
                                 printf("\n \n \t PLAIN TEXt: %s",plain);
                                 printf("\n \n \t ENCRYPTED TEXT: ");
                                 for(i = 0, length = strlen(plain); i < length; i++)
                                 {
                                 cipher[i]=plain[i] + key;
                                if (isupper(plain[i]) && (cipher[i] > 'Z'))
                                 cipher[i] = cipher[i] - 26;
                                 if (islower(plain[i]) && (cipher[i] > 'z'))
                                 cipher[i] = cipher[i] - 26;
```

```
printf("%c", cipher[i]);
}
printf("\n \n \t AFTER DECRYPTION : ");
for(i=0;i<length;i++)
{
plain[i]=cipher[i]-key;
if(isupper(cipher[i])&&(plain[i]<'A'))
plain[i]=plain[i]+26;
if(islower(cipher[i])&&(plain[i]<'a'))
plain[i]=plain[i]+26;
printf("%c",plain[i]);
}
getch();
}
```

OUTPUT:



RESULT:

The main aim is to study the detail report of cyber forensic tools is completed

EXPT.NO 8(B)	Write the step by step procedure for Hiding and extracting any Text file behind an image file using Command Prompt	DATE

AIM:

The main aim is to hide and extract any text file behind an image file using Command Prompt.

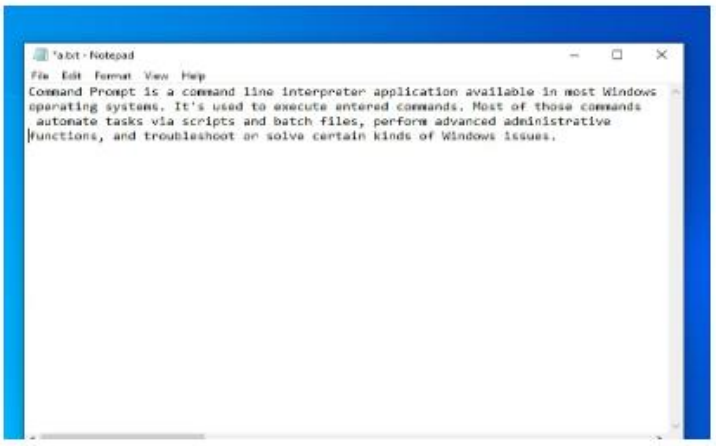
PROCEDURE:

1. Any file like .rar .jpg .txt or any file can be merged inside another file. In a simple way, we shall learn how to hide a text file inside an image file using the Command Prompt.

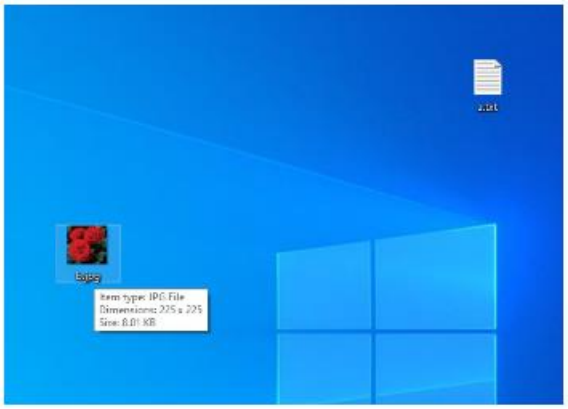
2. Suppose you have to hide a text file “A.txt” with the image file “B.jpg” and combine them in a new file as “C.jpg”. Where “C.jpg” is our output file which contains the text hidden in the image file.

Step1:Create a text document with the file name and .txt as an extension
Example: a.txt is created

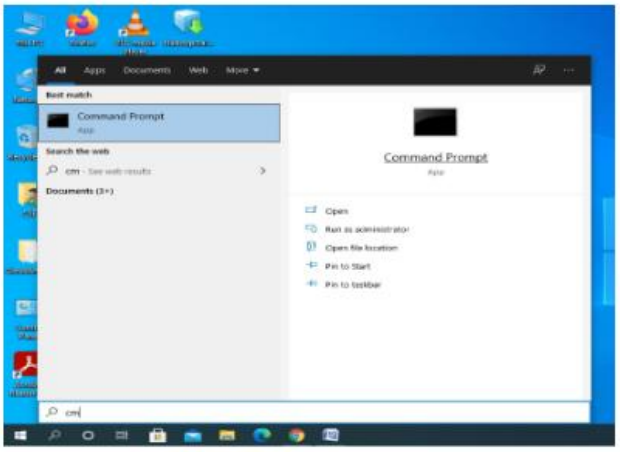
Step2: Type the content which you need to hide in the image and save it



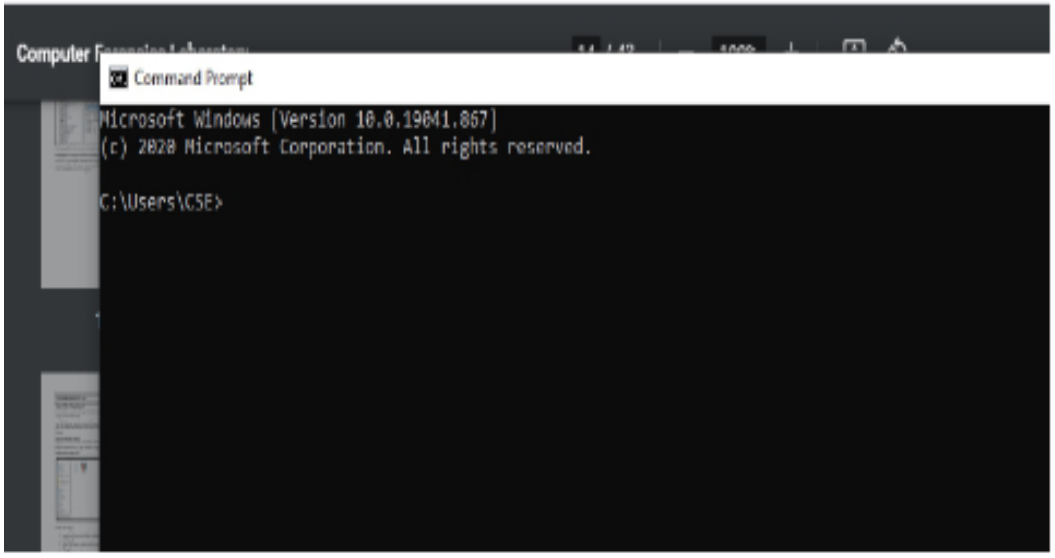
Step 4: Create an image file and save it with the extension .jpg
Example: b.jpg is created



Step 5: Open command prompt by selecting start icon in the task bar

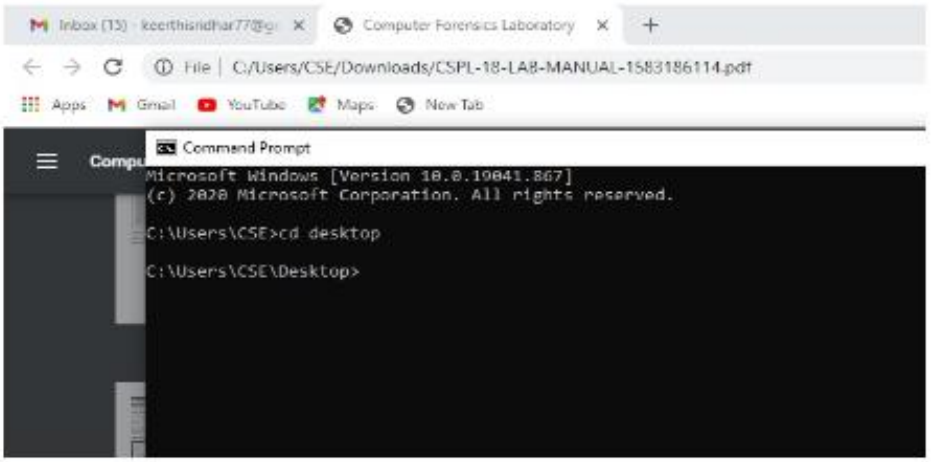


Step 6: Open the command prompt a black working place will be available (or) press ctrl+r and type cmd and hit enter.

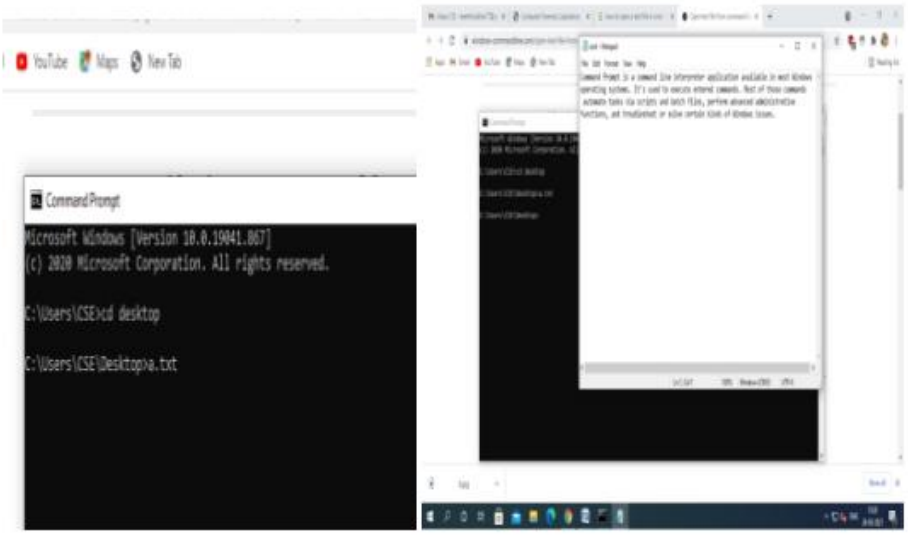


Step 7: Move to the folder where the two are located the CD command is used to enter in to the folder.

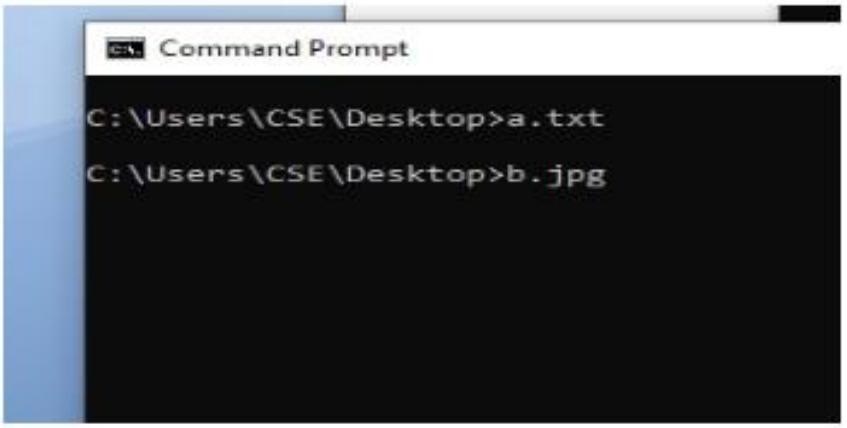
>>cd desktop



Step 8: Open the text file by its file name Example a.txt then txt file will get open

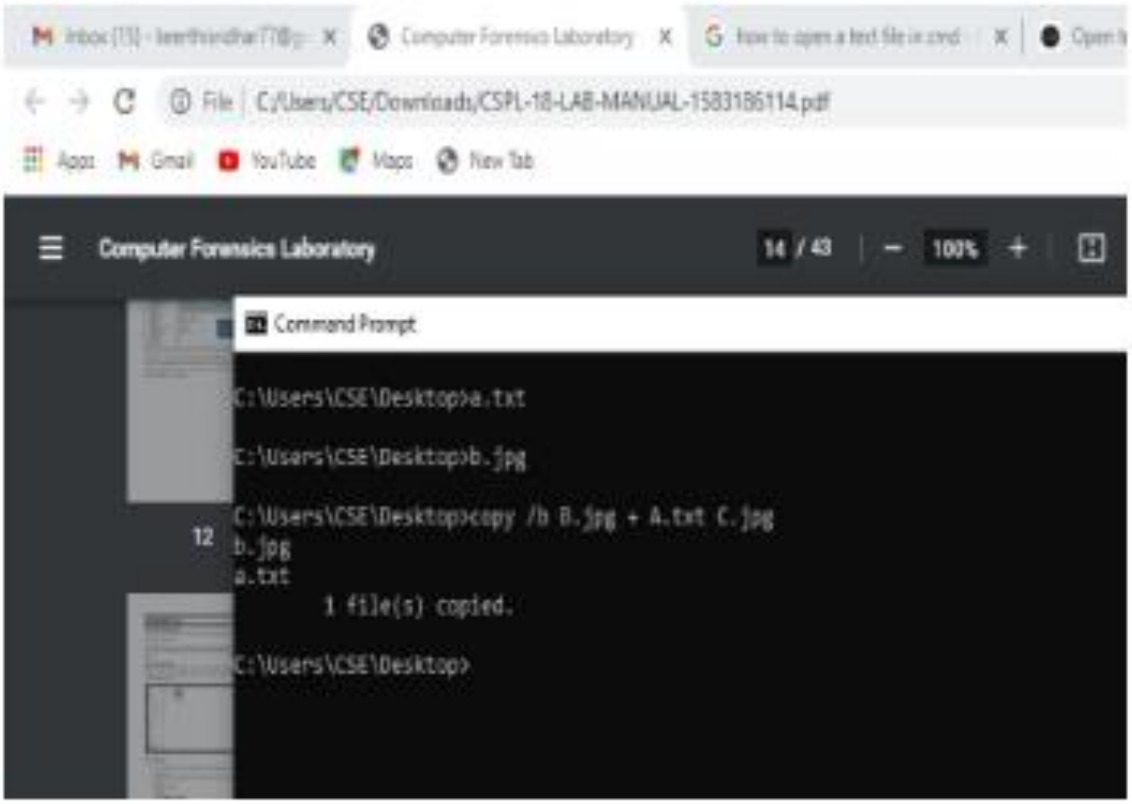


Step 9: Open the .jpg file by its file name Example b.jpg then the image file will get open



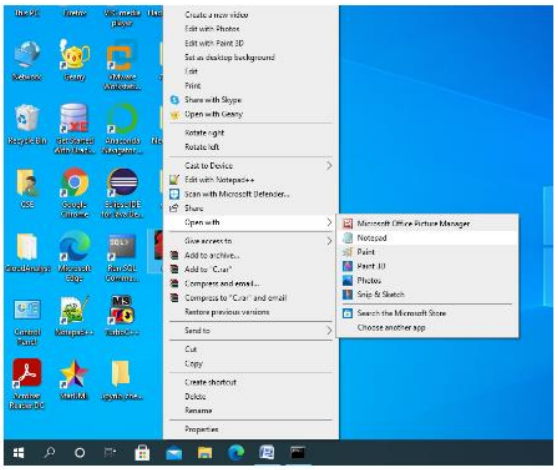
Step 10: Now type the following
Syntax: copy /b Name-of-file-containing-text-you-want-to-hide.txt + Name-of-

initialimage.jpg Resulting-image-name.jpg
Code: > copy /b B.jpg + A.txt C.jpg

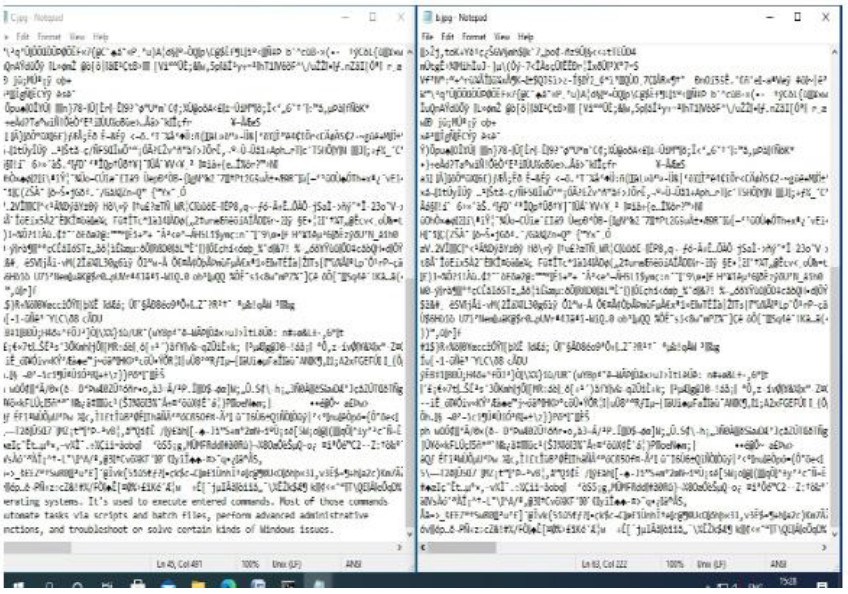


Step 11: locate C.jpg file from where you want to retrieve text data

Step 12: Right-click and open with notepad



Done! Successfully opened! In the last of the notepad, you'll find the content of the text file



RESULT:

The main aim is to hide and extract any text file behind an image file using Command Prompt is completed successfully