DAYANANDA SAGAR College OF ENGINEERING

(An Autonomous Institution affiliated to

Visvesvaraya Technological University, Belgravia)

Department of Computer Science & Engineering

2021-2022

SIXTH SEMESTER

CYBER SECURITY LAB MANUAL

Sub Code: 18CS6DLCSL

DAYANANDA SAGAR COLLEGE OF ENGINEERINGDEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DSCE
DEPARTMENT OF COMPUTER SCIENCE

Vision and Mission of the Department

Vision

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

Mission

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

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

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

* To encourage innovation through multidisciplinary research and development activities

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

DAYANANDA SAGAR COLLEGE OF ENGINEERINGDEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DSCE
DEPARTMENT OF COMPUTER SCIENCE

Code of Conduct in the Lab

Do's

Students shall

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

Don'ts

Students shall not

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

COURSE OBJECTIVES AND COURSE OUTCOMES:

COURSE OBJECTIVES:

1. To be familiar with different types of Tools and methods used in Cyber Crime.
2. To be fluent with various security measures for handling different types of Cyber-attacks.
3. 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	Analyze the apply security vulnerabilities of E -Applications
CO3	Analyze and apply different Cyber Security tools
CO4	Analyze the apply Security issues in windows

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).	1	CO1
	b)	Write the commands to Gather the Information about fragmentation values using Windows Command line Utilities.	2	CO1
2	a)	Write the steps to analyze the security vulnerabilities of E-commerce Services. 1. Vulnerabilities due to Buffer Overflow 2. Vulnerabilities due to Log Forging 3. Vulnerabilities due to Database Servers	1	CO2
	b)	Analyze and scan the System Vulnerabilities using Microsoft Baseline Security Analyzer (MBSA) Tool.	2	CO2
3	a)	Explore different types of techniques used for Web based Password Capturing.	1	CO4
	b)	Write the step by step procedure for Password Cracking on an authorized MS Excel Document.	2	CO4
4	a)	Analyze the problems and its preventive measure of Sniffing attack.	1	CO2
	b)	Explore the Quickstego Tool for Hiding and Recovering the text and image based Information Using.	2	CO4
5	a)	Study of various Cyber Forensic Tools.	1	CO3
	b)	Explore Compare It Tool to Compare of two files for Forensic Investigation.	2	CO3
6	a)	Write the steps to Download a website using Website Copier tool (HTTrack).	1	CO3
	b)	Explore the Snow Tool for hiding the information in Text File.	2	CO3
7	a)	Illustrate the defamation and repairment solution caused by Virus and Trojans.	1	CO2
	b)	Write a program to illustrate Buffer overflow attack.	2	CO2
8	a)	Analyze the Security Issues and Threats in E-Mail Application.	1	CO2
	b)	Write the step by step procedure for Hiding and extracting any Text file behind an image file using Command Prompt.	2	CO4

Text Book:

1.SunitBelapure and Nina Godbole, “Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives”, Wiley India Pvt Ltd, ISBN: 978-81-265-21791, Publish Date 2013.

2. Michael E. Whitman and Herbert J. Mattord,”Principles of Information Security Fourth Edition”, Course Technology, Cengage Learning, ISBN-13: 978-1-111-13821-9, Publish Date 2012.

EXPT.NO 1(A)	Write the 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:

Browser security is an important part in keeping your information safe.

- Your browser is the window to the internet and also the first line of defense against malware threats. Some small tweaks to your browser security settings are all that you need to make your time online that much safer.

Browser features and their security vulnerabilities

- Browsers use many tools for various tasks, such as Java, Flash Player, ActiveX, etc. But these often come with security flaws, which cybercriminals exploit to get access to your PC. A quick rundown of these tools will help you figure out if you need them or not.

Deactivate ActiveX.

- A browser add-on that comes preinstalled on Internet Explorer or Microsoft Edge and only works with these browsers. ActiveX acts as a middle man between your PC and Java/Flash based interactions in certain sites.
- This creates security problems by giving malicious websites a window into your PC. What's more, ActiveX is rarely used nowadays, so be on your guard if a site asks you to install it and accept the installation only if you are 150% sure that site is trustworthy.

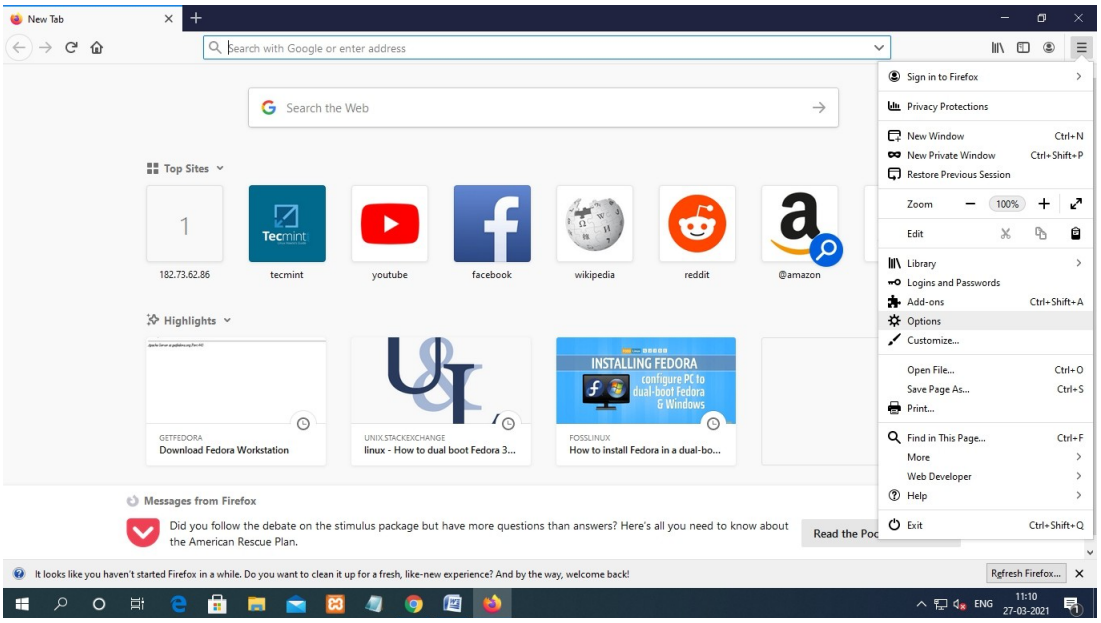
Try to disable JavaScript.

- JavaScript is a programming language used by websites to run various programs and features. Sites such as YouTube or Google Docs need it to function, but so do advertising, pop-up software and a whole host of other spam my elements from the internet.
- Cybercriminals use JavaScript in malicious ways in order to infect your device with malware and other harmful software.
- If you disable JavaScript altogether you will get a much quicker and simplified browser experience, with little to no ads, pop-ups, greatly improved page load times and generally a cleaner Internet experience at the cost of specialized tools such as Google Docs or YouTube.

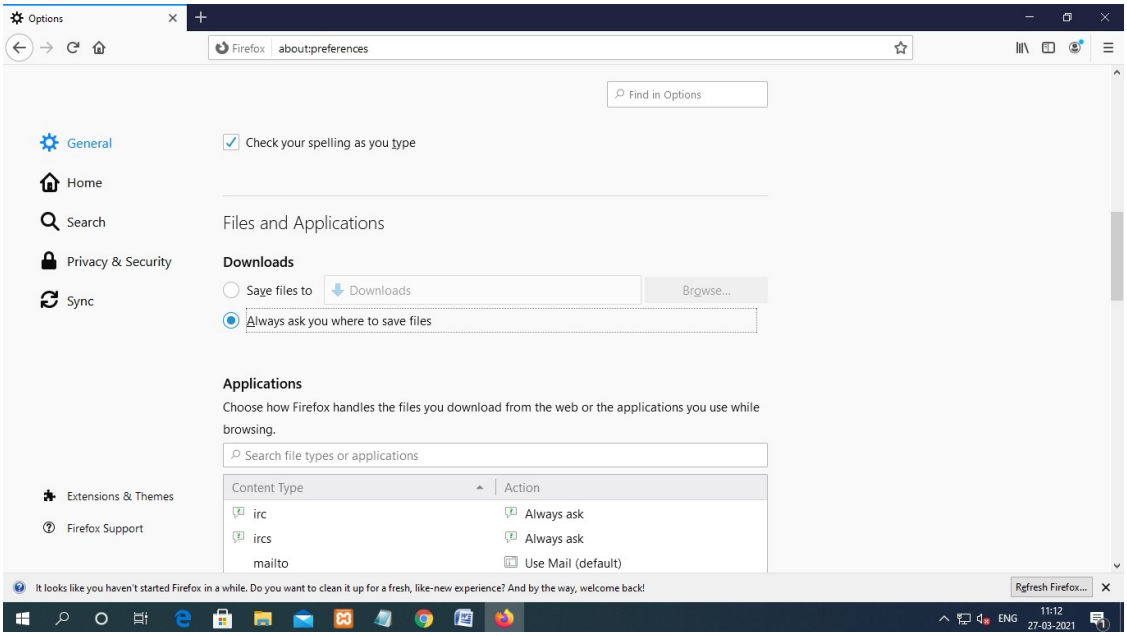
- This doesn't need to be as drastic as it sounds, since browsers do allow you to white list certain sites which can run JavaScript. Delete Cookies.
- These are small data files stored on your browser. Websites use cookies in order to remember your accounts and passwords, browsing history and to track user behavior on their site.
- Because of the information they contain, cookies are prime targets for cybercriminals, especially the ones that contain emails, account names and passwords.
- When you disable and clear cookies you cut down on the personal data cybercriminals can obtain. One thing you will want to keep in mind is that there are two types of cookies: First party and third party cookies.
- First party cookies are placed by the site you visit, for instance you get a first party cookie by cnn.com while visiting cnn.com.
- Third party cookies are placed by other sites, for example you get a cookie from amazon.com while visiting cnn.com.
- First party cookies are frequently used to remember your login information so you don't have to enter it every time you visit a site.
- But we can't stress this enough, don't allow your browser to save passwords! Third party cookies are almost always placed on your computer by advertisers or marketers interested in tracking your movement online, so nothing bad will happen if you block them.
- Browser extensions and add-ons add extra functionality to your browser such as ad blocking or search bars. However, these add-ons pose a security risk, since they can open up windows into your PC which can be exploited to inject malware.

Firefox hacks and tips for better security

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

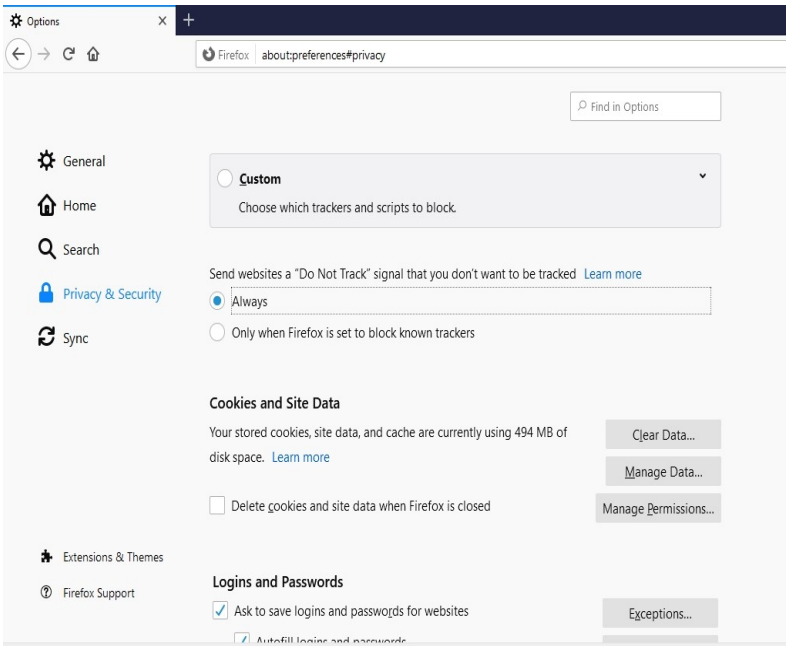


In the “General” tab, at the Downloads section, press “Always asks me where to save files”. This way, you won’t have a web location try to automatically save dangerous content to your computer.



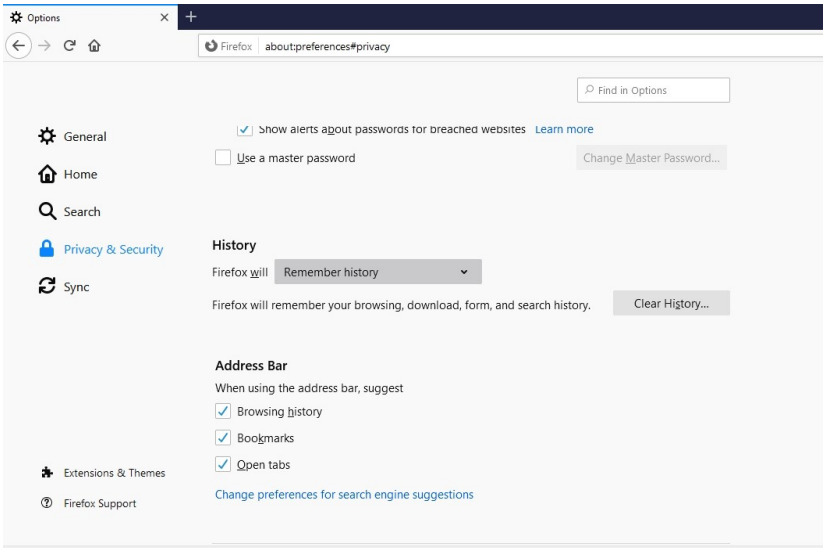
At the same time, this gives you the option to place suspicious content in a safe location where you can analyze it afterwards.

Next, go to the Privacy tab.



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

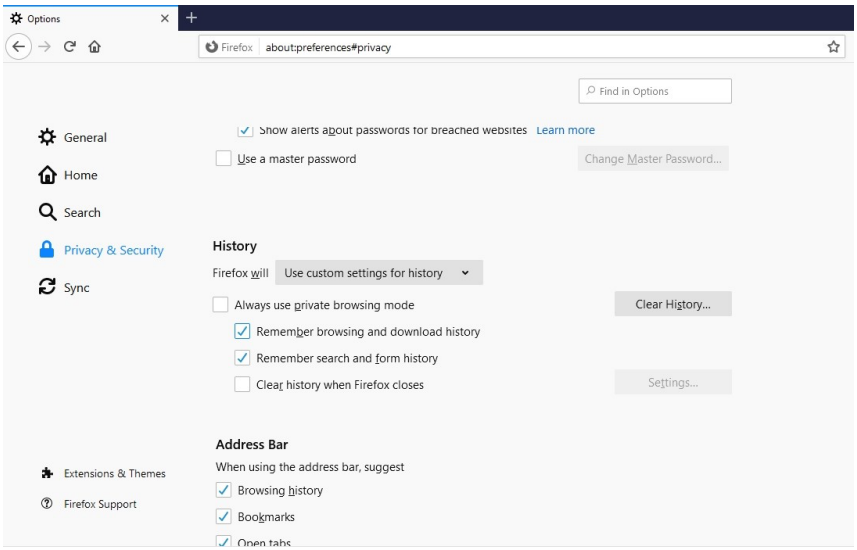
After you do this advertising, commerce and various other sites shouldn't be able to track you across the web. While in the Privacy tab, at the "History" section, choose



"Firefox will never remember history".

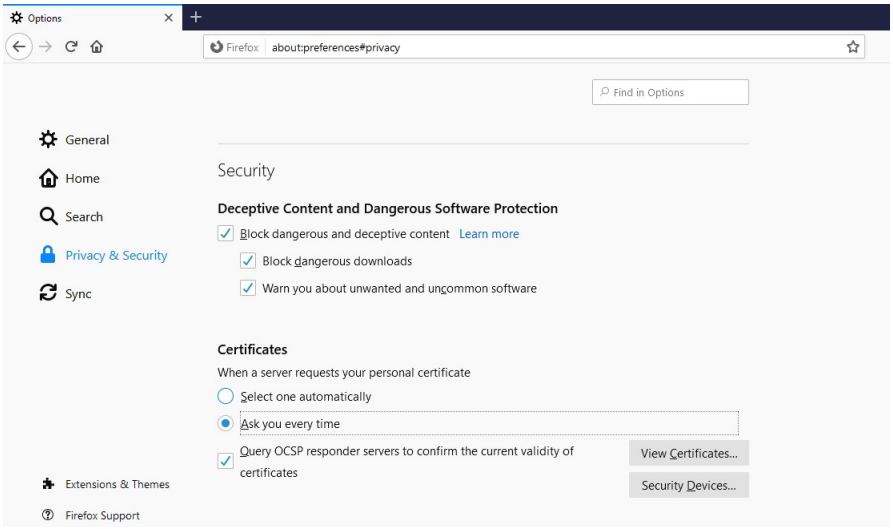
This is especially important if you know your device may be used by other people.

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



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

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



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

RESULT:

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

EXPT.NO 1(B)	Write the commands to Gather the Information about fragmentation values using Windows Command line Utilities.	DATE:

AIM:

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

PROCEDURE:

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

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

Topology Diagram:

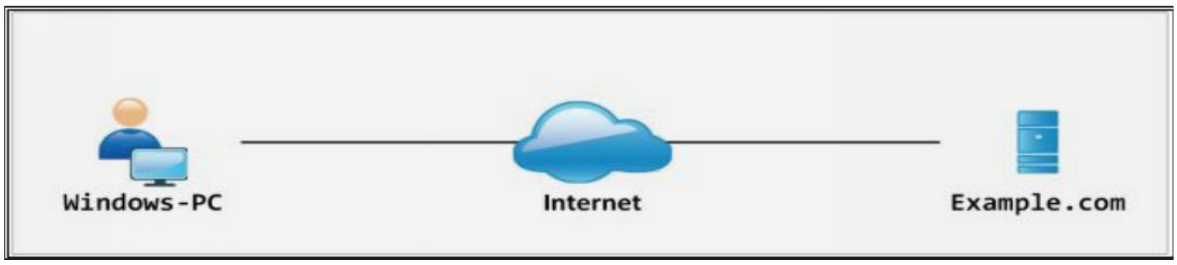
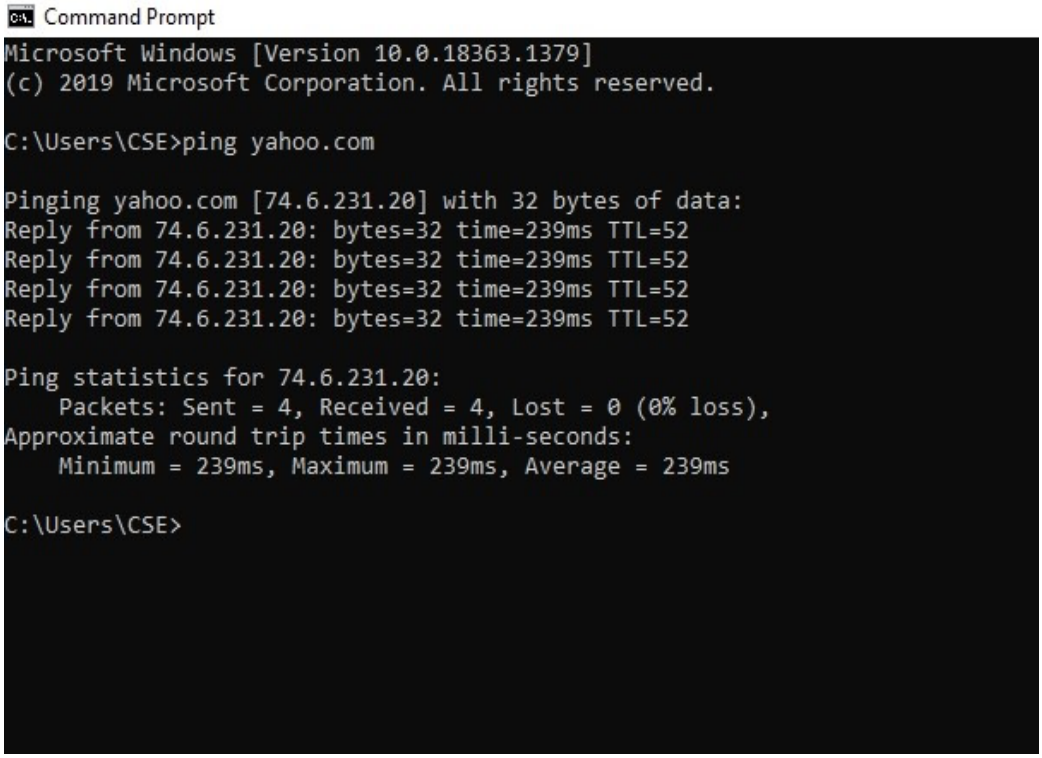


Figure: Topology Diagram

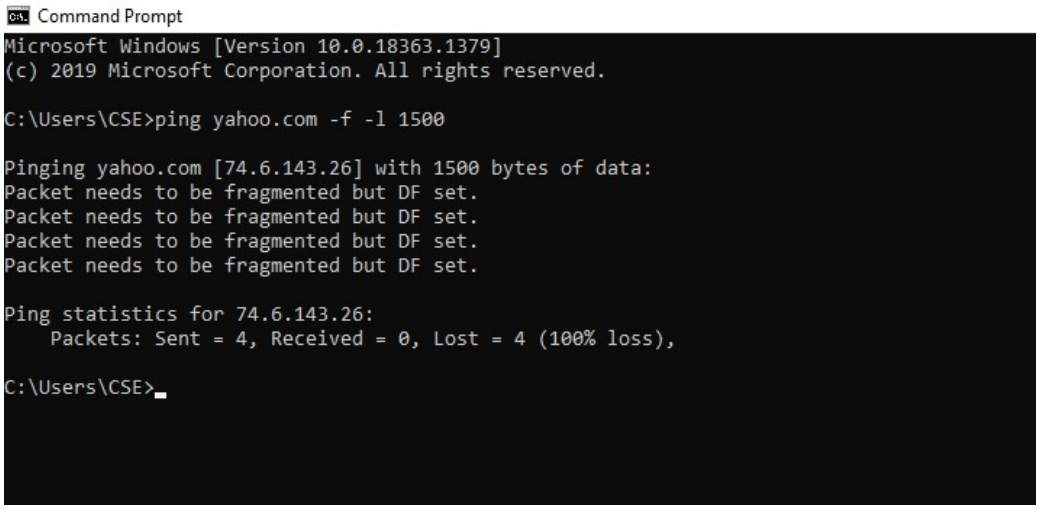
1) Open Windows Command Line (cmd) from Windows PC.
2) Enter the Command “ping yahoo.com” to ping.



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

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

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



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

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

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

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

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

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

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

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

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

RESULT:

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

EXPT.NO 2(A)	Write the steps to analyze the security vulnerabilities of E-commerce Services. 1.Vulnerabilities due to Buffer Overflow 2.Vulnerabilities due to Log Forging 3.Vulnerabilities due to Database Servers	DATE:

AIM:

The main aim is to analyze the security vulnerabilities of e-commerce services.

PROCEDURE:

Vulnerabilities due to Buffer Overflow:

- A buffer overflow condition occurs when a program attempts to copy more data in a buffer than it can hold. Buffer overflow is probably the best known form of software security vulnerability.
- At the code level, buffer overflow vulnerabilities usually involve the violation of a programmer's assumptions. Hackers use buffer overflows to corrupt the execution stack of a web application.
- Buffer overflow flaws can be present in both the web server or application server products that serve the static and dynamic aspects of the site. Buffer overflows generally resulted in to crashes.
- Other type of attacks will create the situation like lack of availability are possible, including putting the program into an infinite loop.

Vulnerabilities due to Log Forging:

- Writing invalidated user input to log files can give access to attacker for forging log entries or injecting malicious content into the logs.
- Log forging vulnerabilities occur in following conditions: i) Data copied to an application from an unreliable source. ii) The data is copied to an application or system log file. Applications uses log file to store a history of events for later review and record, statistics gathering, or debugging.
- Analysis of the log files may be misdirected if an attacker can supply inappropriate data to the application. In the most common case, an attacker may be able to insert false entries into the log file by providing the application with input that includes appropriate characters.
- If the log file is processed automatically, the attacker can render the file unusable by corrupting the format of the file or injecting unexpected characters. A more dangerous attack might involve changing the log file statistics.

Vulnerabilities in database servers:

There are various techniques to attack a database. External attacks may exploit configuration weaknesses that expose the database server. Also weak and insecure Web application can be used to exploit the database. An application with excess privilege in the database can put database at risk. The main threats to a database server are:

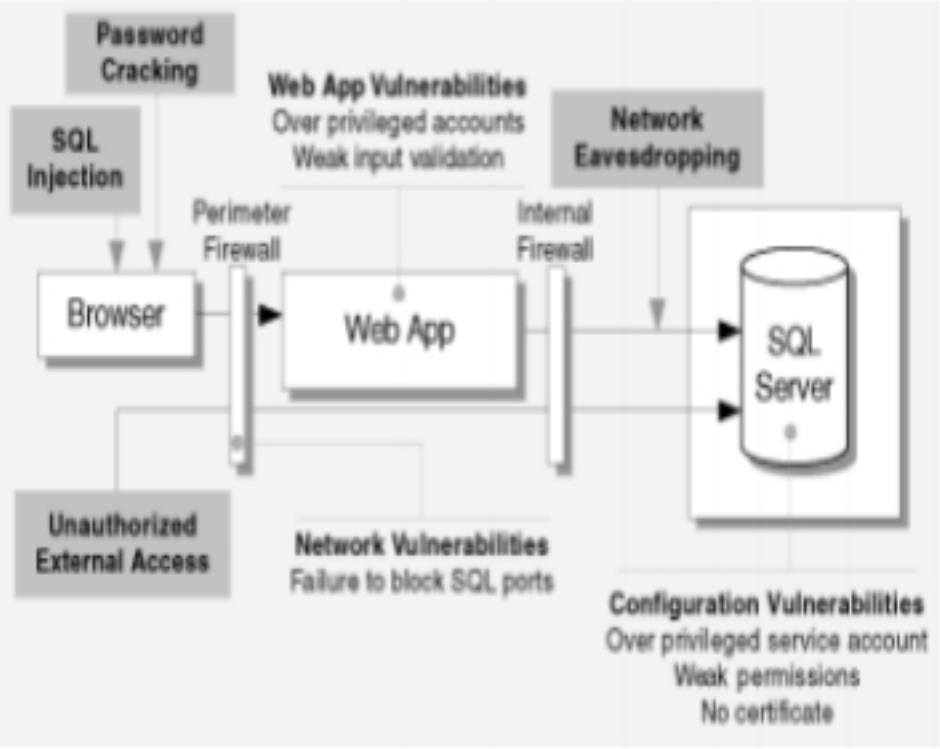


Figure: Main threats to a database server

- **SQL injection:** Technique used to attack database through website entry fields.
- **Network eavesdropping**: It is a network level attack consisting of capturing packets from the networked computers.
- **Unauthorized server access:** Attacked made unauthorized access through various loopholes in the system such as O/S, non availability of firewall etc.
- **Password cracking:** Technique of recovering password from data stored in computer.

RESULT:

The main aim is to analyze the security vulnerabilities of e-commerce services is successfully completed

EXPT.NO 2(B)	Analyze and scan the System Vulnerabilities using Microsoft Baseline Security Analyzer (MBSA) Tool.	DATE:

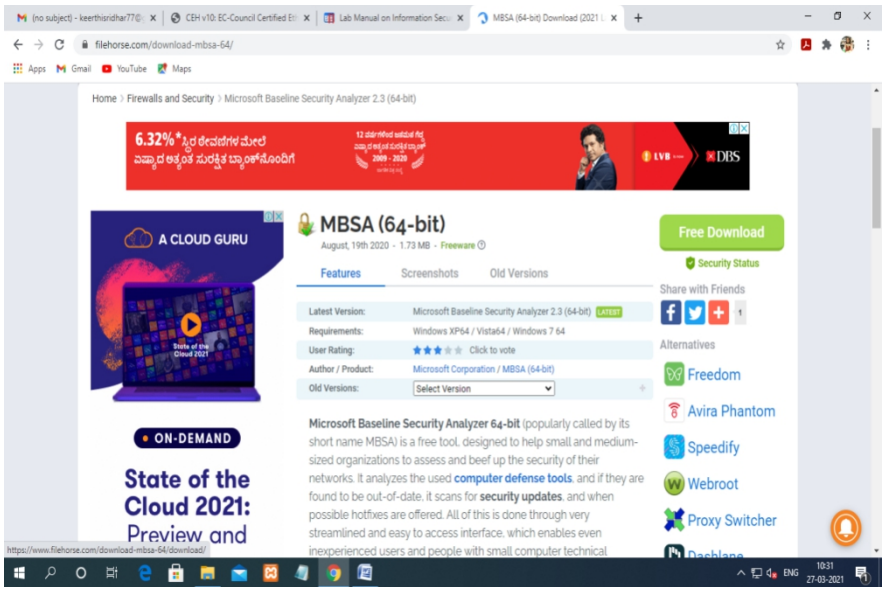
AIM:

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

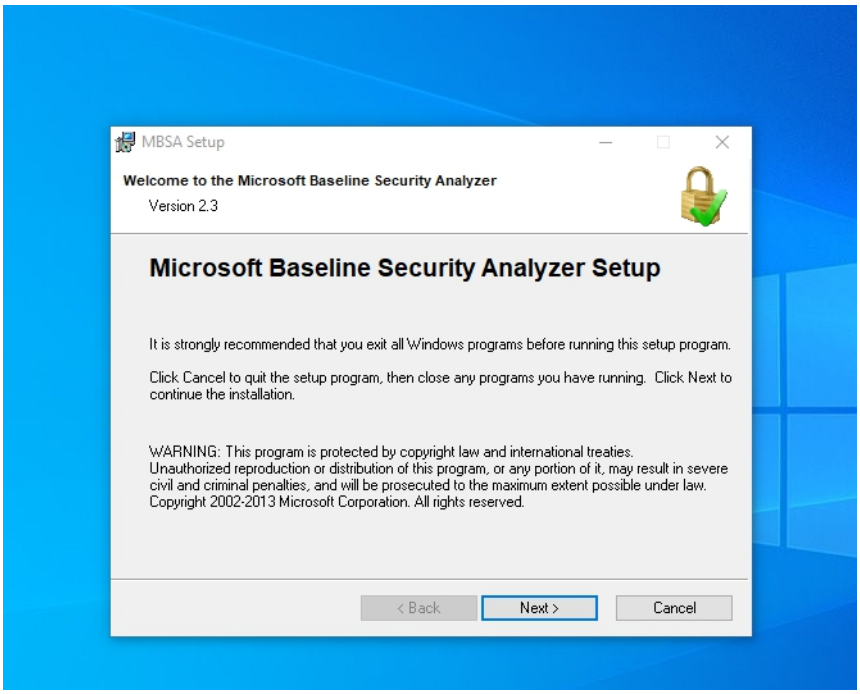
PROCEDURE:

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

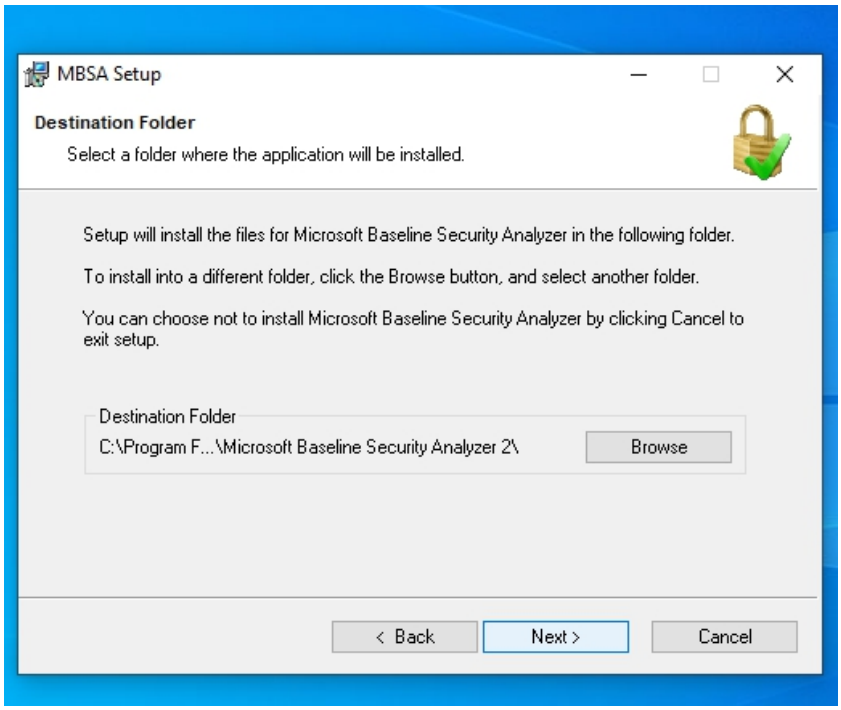
Step 1: download the Microsoft Baseline Security Analyzer (MBSA)



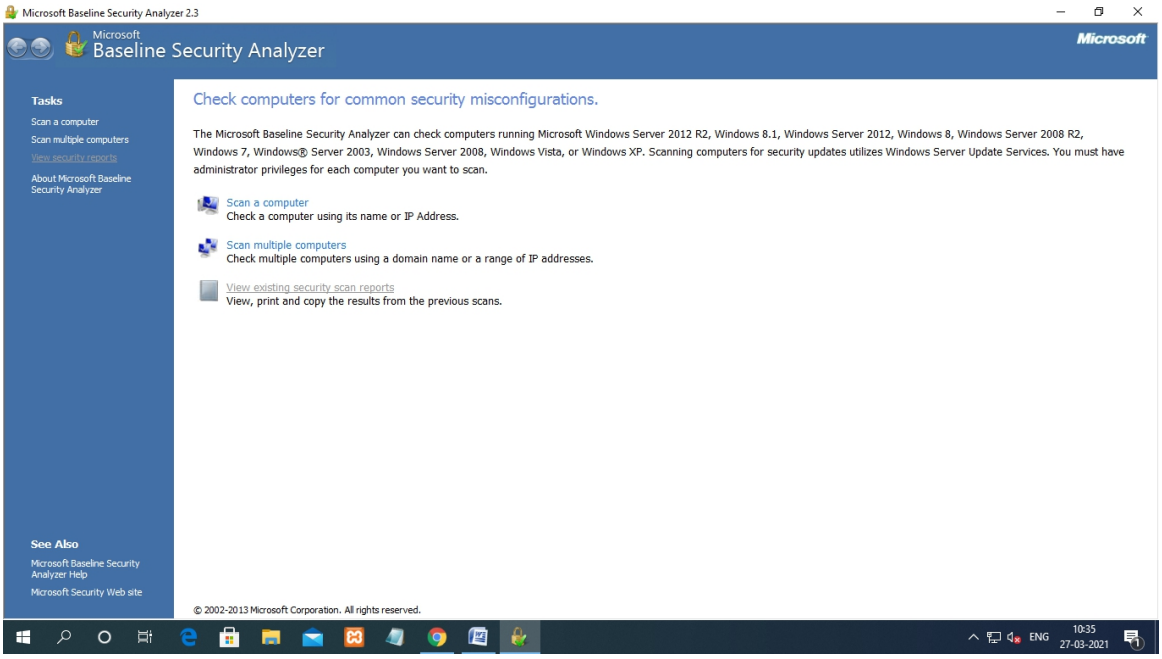
Step2: start and install the Microsoft Baseline Security Analyzer (MBSA) click next to start install



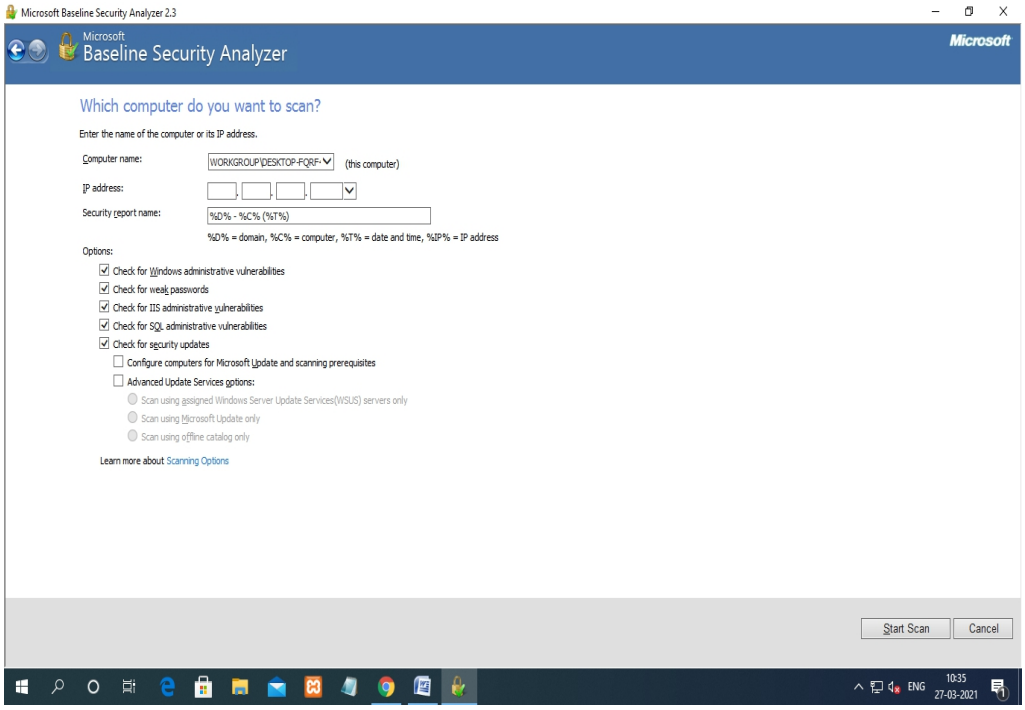
Step3: choose the location to install MBSA



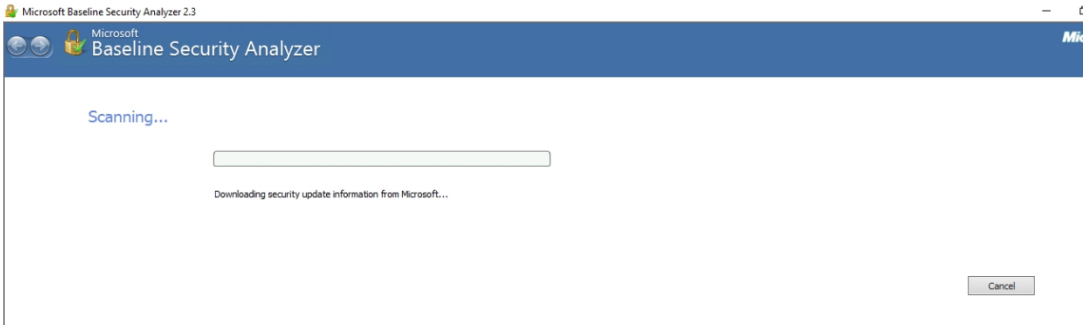
STEP 4:click the scan a computer to start the MBSA



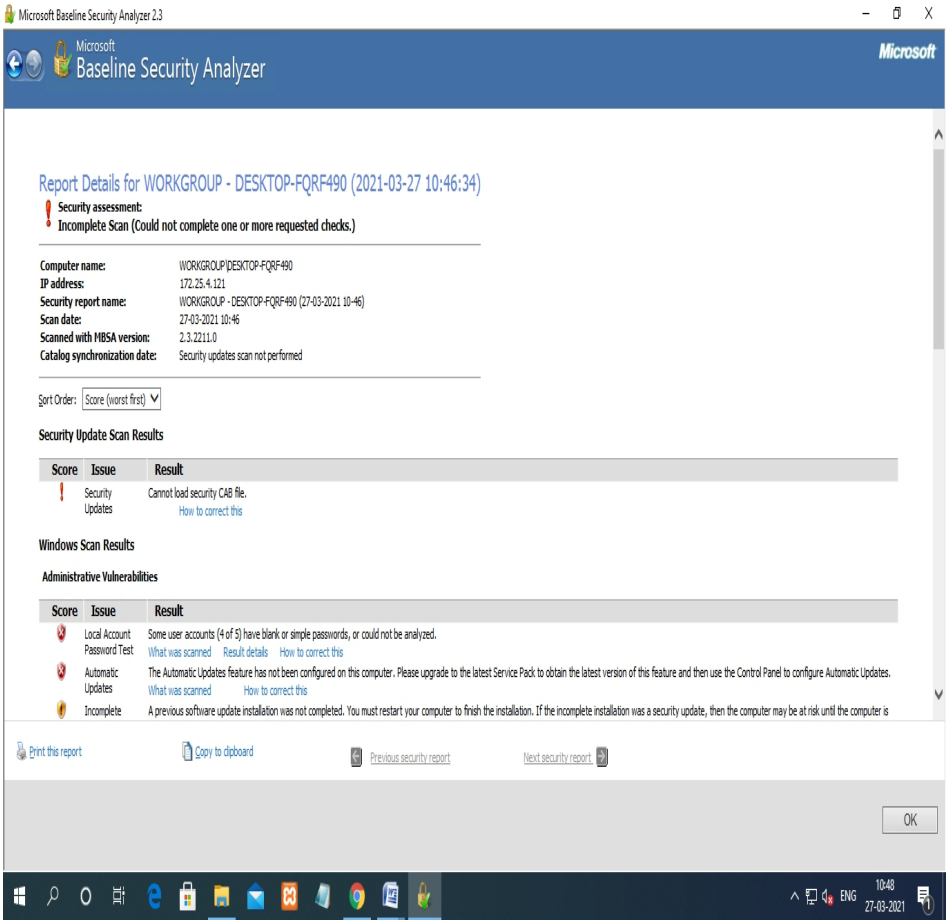
Step 5: provide the IP address and click start scan



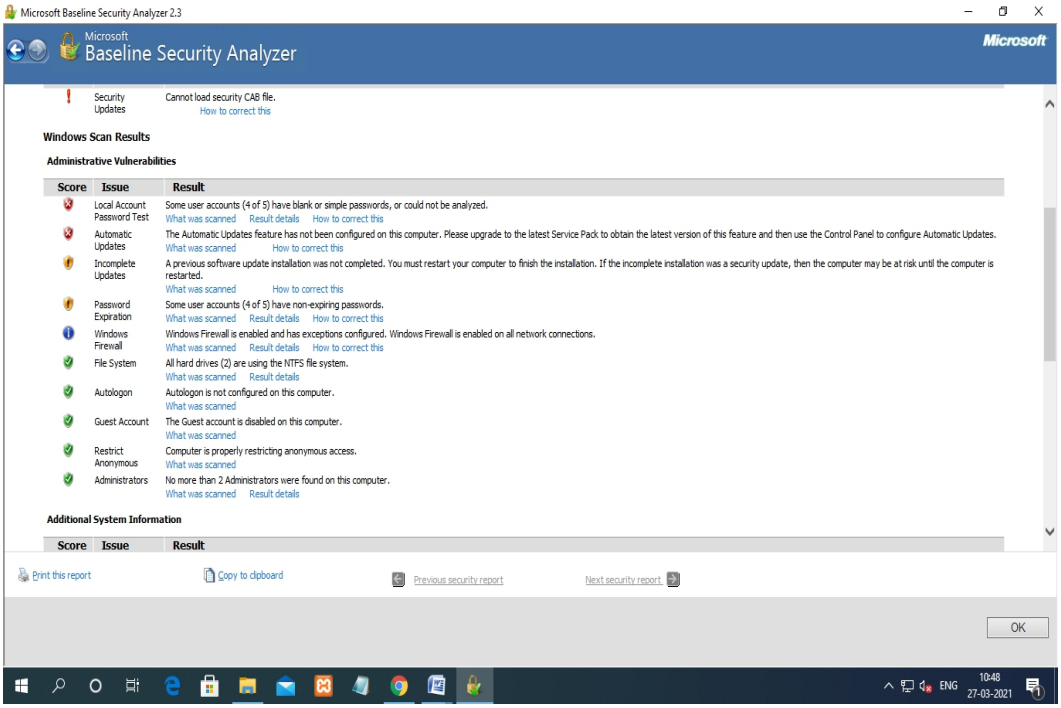
Step 7: The scanning process is GET STARTED



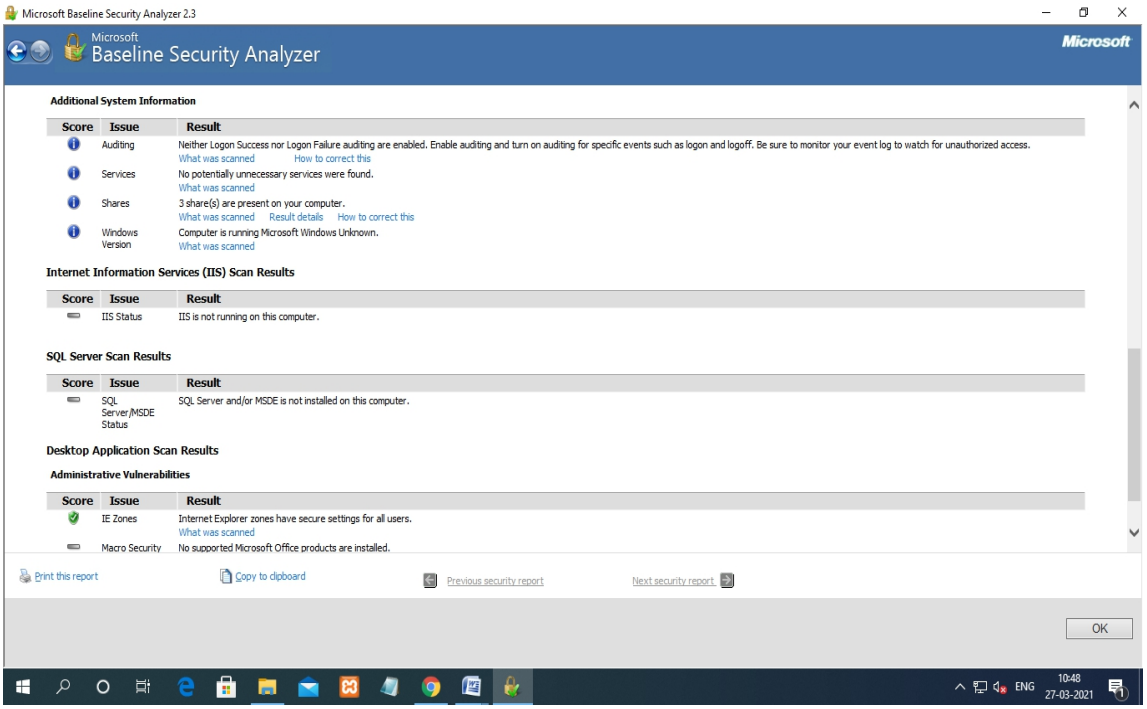
STEP 8: The detail report is generated for the system



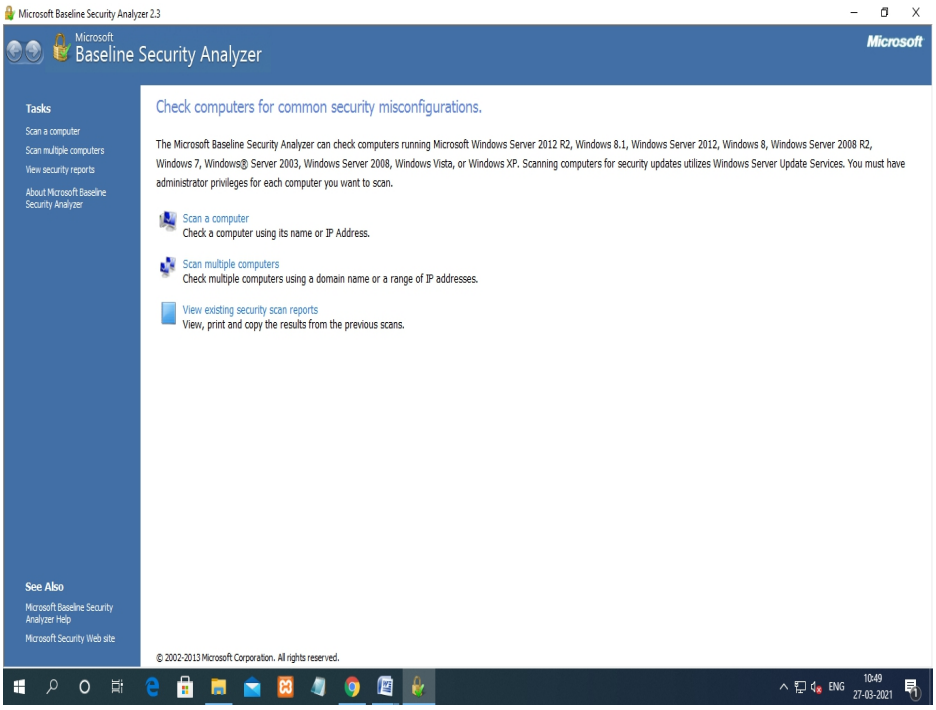
Result about the administrative vulnerabilities



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



And also we can view the existing scan report



RESULT:

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

EXPT.NO 3(A)	Explore different types of techniques used for Web based Password Capturing	DATE:

AIM:

The main aim is to study of techniques uses for web based password capturing in detail.

PROCEDURE:

- The main aim is to Study about Techniques uses for Web Based Password Capturing.
- Many people don't understand how easy it is for attackers to take advantage of weak passwords, and therefore don't use a password manager or other means to make their passwords stronger.
- This post describes 9 common ways passwords get captured, roughly ordered from most to least common. Proper use of a password manager can thwart some of these attacks and limit damages from most other types of attacks.

1: Mass Theft of Password Files:

- Most people don't realize that user names and passwords routinely get stolen while your computer is off and disconnected from the internet. How? Web sites with many users and weak security are prime targets for attackers who want to steal a password file which lists all user names and passwords.
- Recent examples include Monster.com and RockYou.com. While most sites do not store passwords as clear text, many sites store passwords in a form that can be read using widely available rainbow table software. For people who use the same password on many sites, the theft of this password on one site can be the starting point for an attack on all of your accounts.

Protection:

A simple and effective defense for users is to only use long, randomly generated passwords. How long? 15 characters. Rainbow tables easily crack passwords 8 or fewer characters long and in some cases up to 14 characters.

Damage Control:

In the unlikely case that a rainbow table attack manages to crack one of your 15 character passwords, at least your damages will be limited to one account if you have a unique password for each account. Change the password of any account that becomes compromised due to mass theft.

2: Brute Force:

- Brute Force refers to discovering passwords through trial and error, similar to trying every possible combination on a lock. The most well known form of

brute force attack is for password cracking software to methodically try millions of passwords on one specific user name on a specific account.

- A typically weak password can be cracked in less than a day using this method. Security conscious online vendors like banks or e-mail services provide some protection against such brute force attempts by denying access if there are too many attempts per hour. However, different forms of brute force can be used to get around these safeguards. A common example is software which automatically logs in to millions of different accounts per day by combining popular user names, passwords, and web sites (i.e. try password1 at Jsmith@gmail.com, 123456 at dj@facebook.com, QWERTY at Mrodriguez@yahoo.com, etc.).
- As such methods become more widely adopted, it would not be surprising if nearly all accounts with short user names and short passwords get compromised. Brute force is also used as a supplementary attack after a first password is captured. For example, if the password badpassword1 was captured by phishing, brute force can be used to try similar passwords on other accounts. Protection: Brute force attacks are highly unlikely to crack very strong passwords. So just use strong passwords. I suggest randomized 15 character jumbles. Damage Control: Your damages are limited to one account if you have a unique password for each account. Immediately change the password of the affected account.

3: Eavesdropping: Keystroke Logger on Your Browser

- Many people believe that nothing bad can happen to people who only visit safe, well respected sites. They are wrong. Malicious JavaScript can be injected into any browser on any system, visiting any web site. Keystroke logging is something that is done by some of these JavaScript injections. In most browsers, malicious JavaScript can log keystrokes in all open tabs, until the browser is closed. Usernames and passwords entered during the session can be captured this way.

Protection:

Keystroke logging via browser is growing more common but is unfortunately one of the more difficult threats to defend against. Defenses include: Use Firefox in conjunction with the No Script extension. While this is a strong defense, the overall complication of using No Script (popup, white lists, and blacklists) is more of a hassle than the average Joe wants to deal with. Some security suites attempt to defend against this threat with browser plug-ins, but

these can dramatically slow down browsing. A simpler option is to only access the internet using the Google Chrome browser, which is designed so that malicious JavaScript can be theoretically contained to a single tab. At least other tabs will be safe. Some password managers such as RoboForm enter passwords and usernames in a way which most JavaScript keystroke loggers cannot intercept. None of these suggestions are sure to stop browser-based keystroke loggers, but if you implement one or more of these suggestions you'll at least reduce your chances of getting your usernames and passwords logged by malicious JavaScript. The only perfect defense is to not connect to the internet at all.

Damage Control:

Your damages are limited to logins captured while browsing, so long as you have a unique password for each account. Immediately change the password of the affected accounts. If using a browser-based or web-based password manager, you should also change your master password.

4: **Eavesdropping: Public Wi-Fi Monitoring**

- Passwords are frequently stolen on public computers and over public Wi-Fi connections, using free Wi-Fi traffic monitoring software that is simple to operate.

Protection:

Never log in to online accounts using a public computer. When using open Wi-Fi hot spots, you should only log in with your own notebook with services that enforce secure logins and sessions (HTTPS), perhaps using the Firefox Add-on HTTPS Everywhere to help. It is far safer to access email and other accounts using your phone data service, if you have one.

Damage Control:

If you discover that this type of attack has occurred, then you will need to change the password for all of your accounts as well as your master password. If you know exactly when the attack occurred, you can change passwords only for the accounts you used during that session.

RESULT:

The detail Study about Techniques uses for Web Based Password Capturing is completed

EXPT.NO 3(B)	Write the step by step procedure for Password Cracking on an authorized MS Excel Document	DATE:

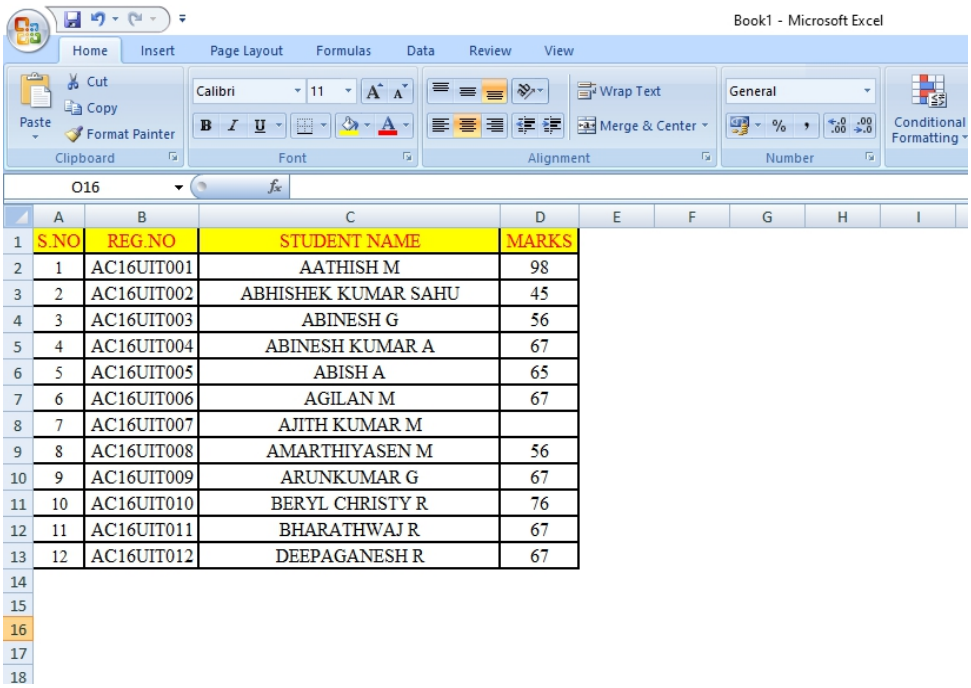
AIM:

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

PROCEDURE:

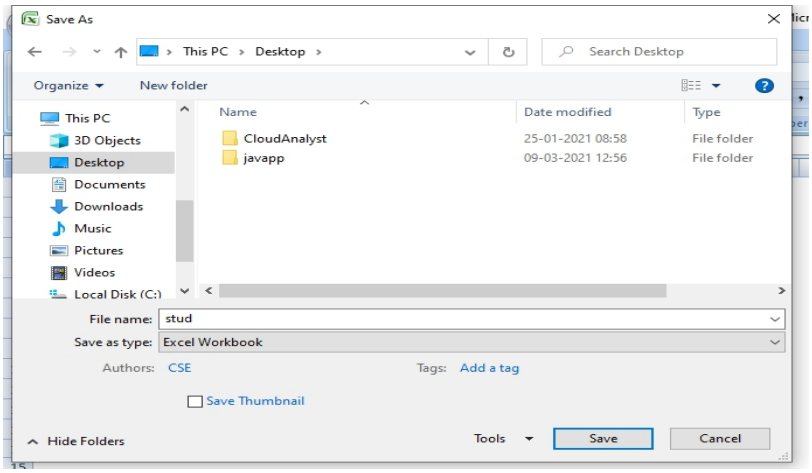
Step 1: Open the MS EXCEL by clicking start menu icon in the task bar.

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

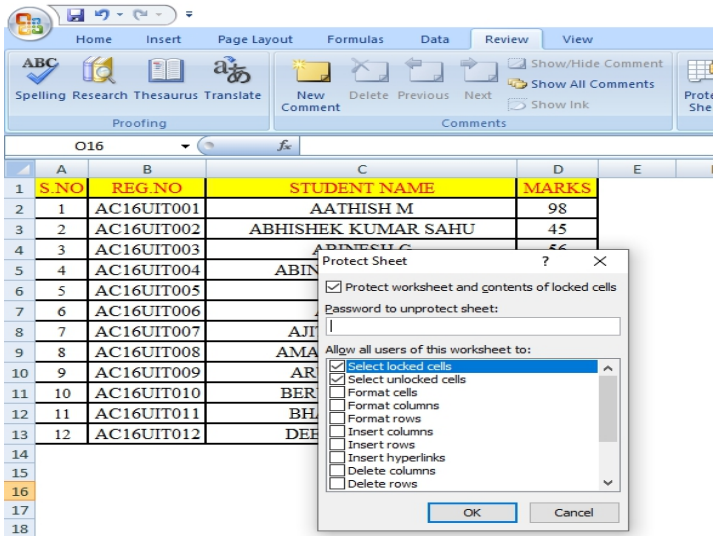


	A	B	C	D	E	F	G	H	I
1	S.NO	REG.NO	STUDENT NAME	MARKS					
2	1	AC16UIT001	AATHISH M	98					
3	2	AC16UIT002	ABHISHEK KUMAR SAHU	45					
4	3	AC16UIT003	ABINESH G	56					
5	4	AC16UIT004	ABINESH KUMAR A	67					
6	5	AC16UIT005	ABISH A	65					
7	6	AC16UIT006	AGILAN M	67					
8	7	AC16UIT007	AJITH KUMAR M						
9	8	AC16UIT008	AMARTHIYASEN M	56					
10	9	AC16UIT009	ARUNKUMAR G	67					
11	10	AC16UIT010	BERYL CHRISTY R	76					
12	11	AC16UIT011	BHARATHWAJ R	67					
13	12	AC16UIT012	DEEPAGANESH R	67					
14									
15									
16									
17									
18									

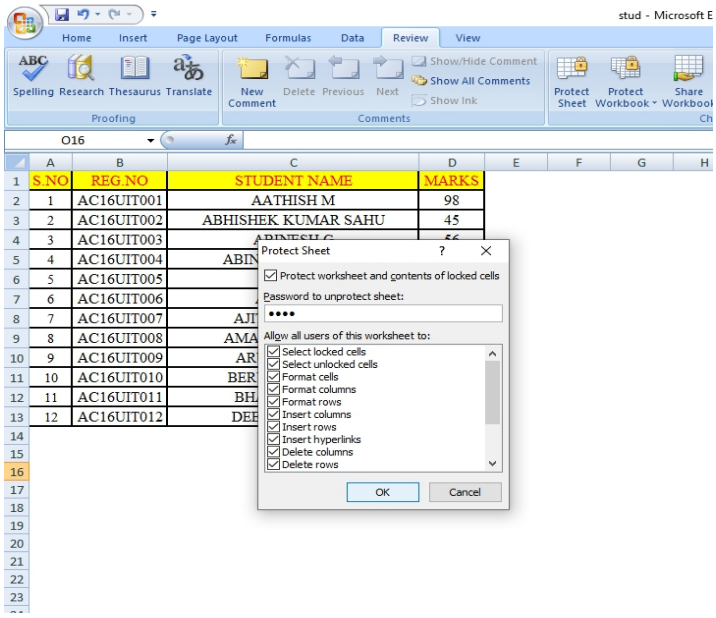
Step 3: Save the MS EXCEL document with a file name and with the extension of .xsls



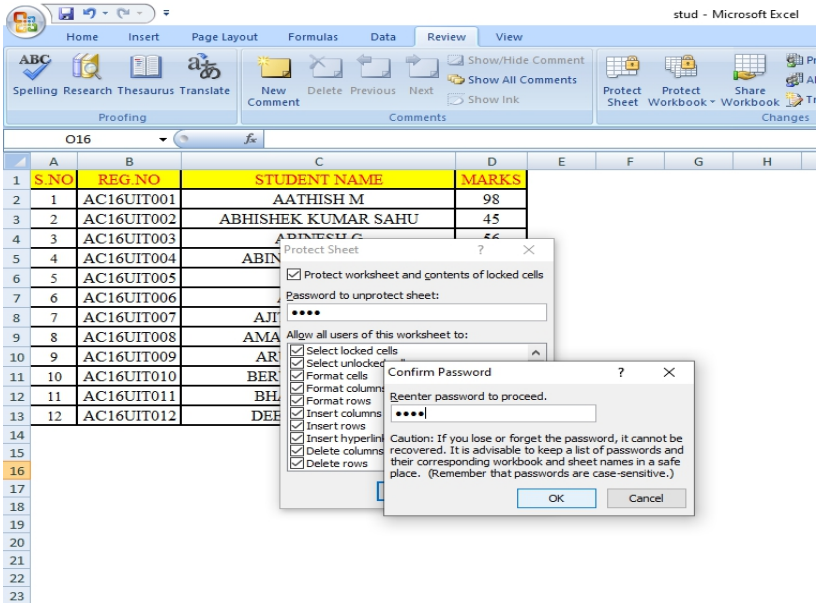
Step 4: Protect your document with a password by selecting review tab and choose protect sheet. Assign a password



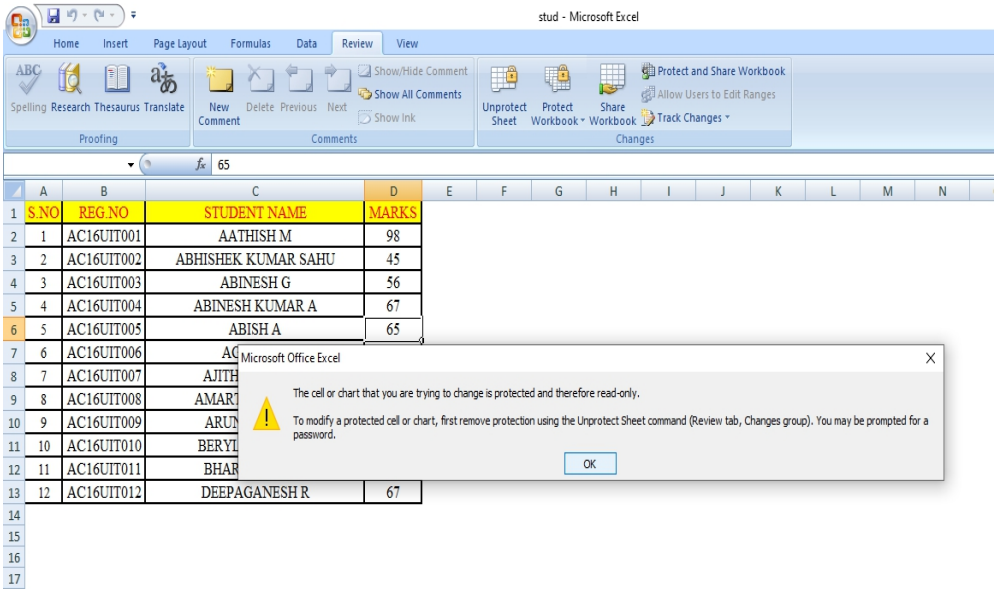
Step 5: Enable all the alignment edition option so therefore one can edit out official document. Select ok



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

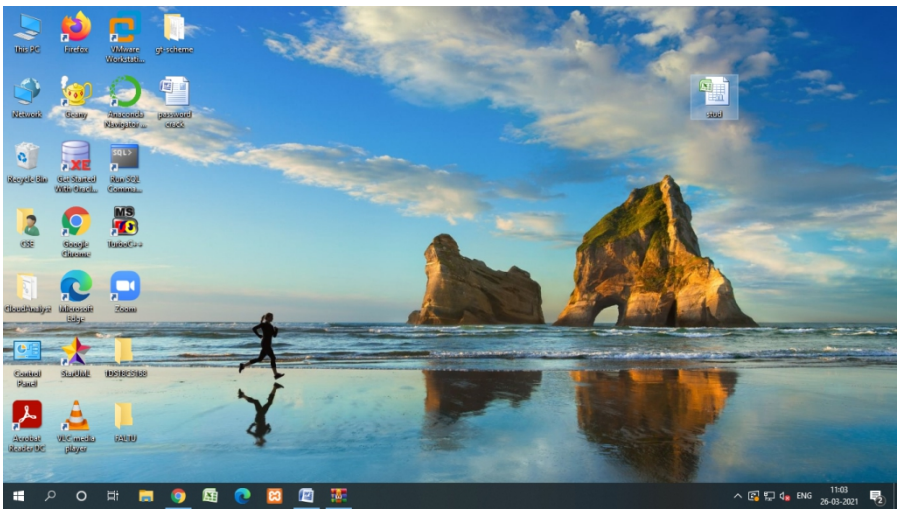


Step 7: Now check if the editing is possible in our official document. If we try to change any this will display that this document is protected by password

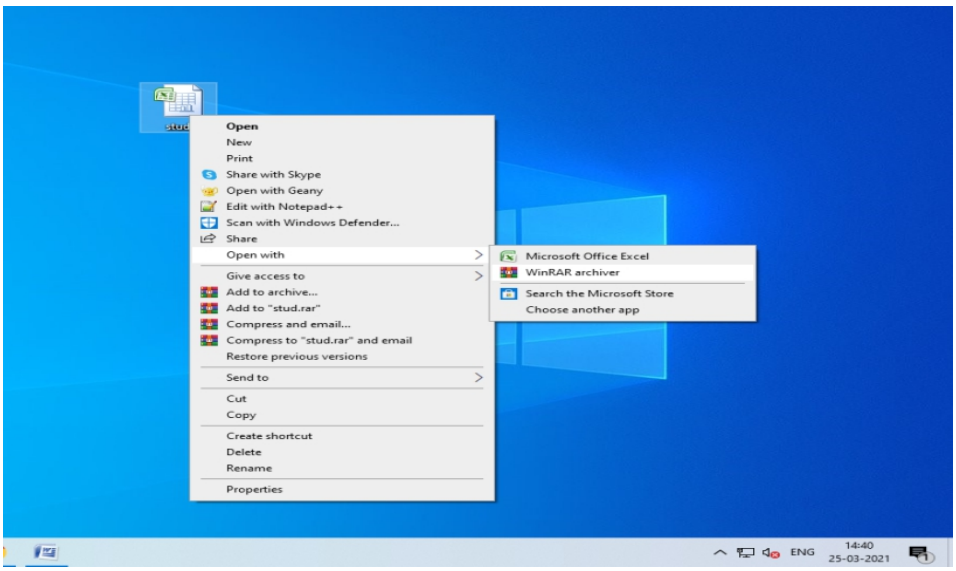


S.NO	REG.NO	STUDENT NAME	MARKS
1	AC16UIT001	AATHISH M	98
2	AC16UIT002	ABHISHEK KUMAR SAHU	45
3	AC16UIT003	ABINESH G	56
4	AC16UIT004	ABINESH KUMAR A	67
5	AC16UIT005	ABISH A	65
6	AC16UIT006	AC	
7	AC16UIT007	AJITH	
8	AC16UIT008	AMART	
9	AC16UIT009	ARUN	
10	AC16UIT010	BERYL	
11	AC16UIT011	BHAR	
12	AC16UIT012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

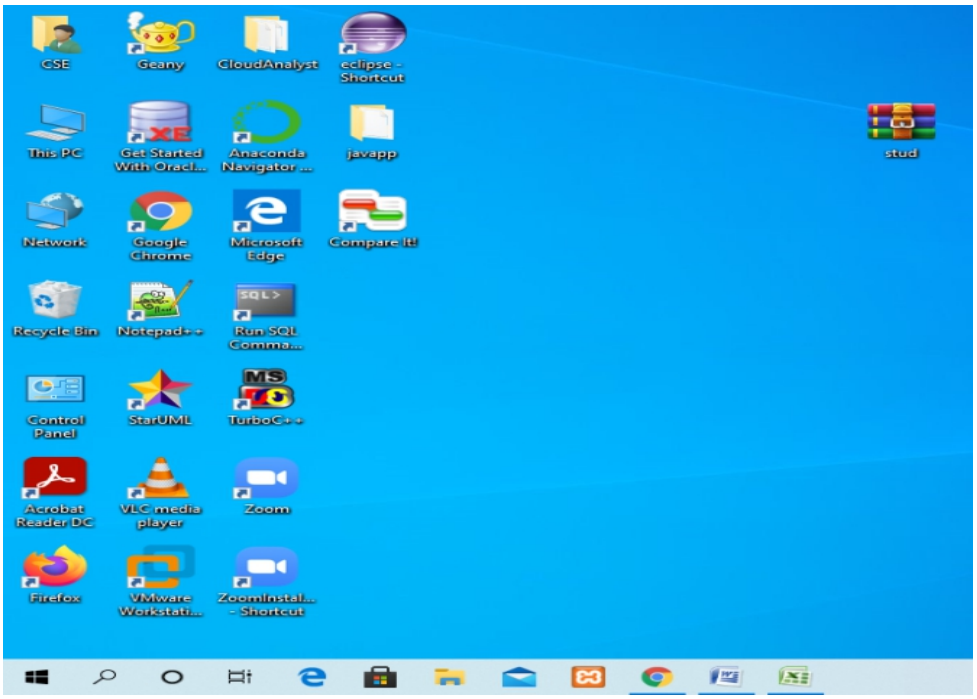
Step 8: Save the document in a new folder or in a desktop



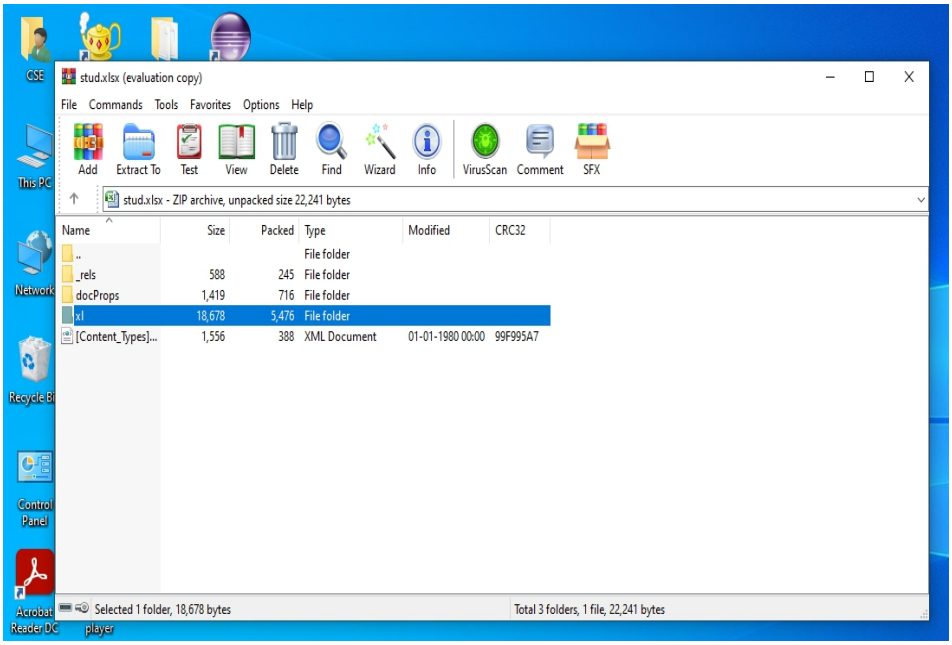
Step 9: Select the file and change the extension as .zip or right click on the file select the properties form the pop-up menu and change the extension of the document otherwise right click on the file select open with and choose winRAR. The .xsls file is changed to .zip



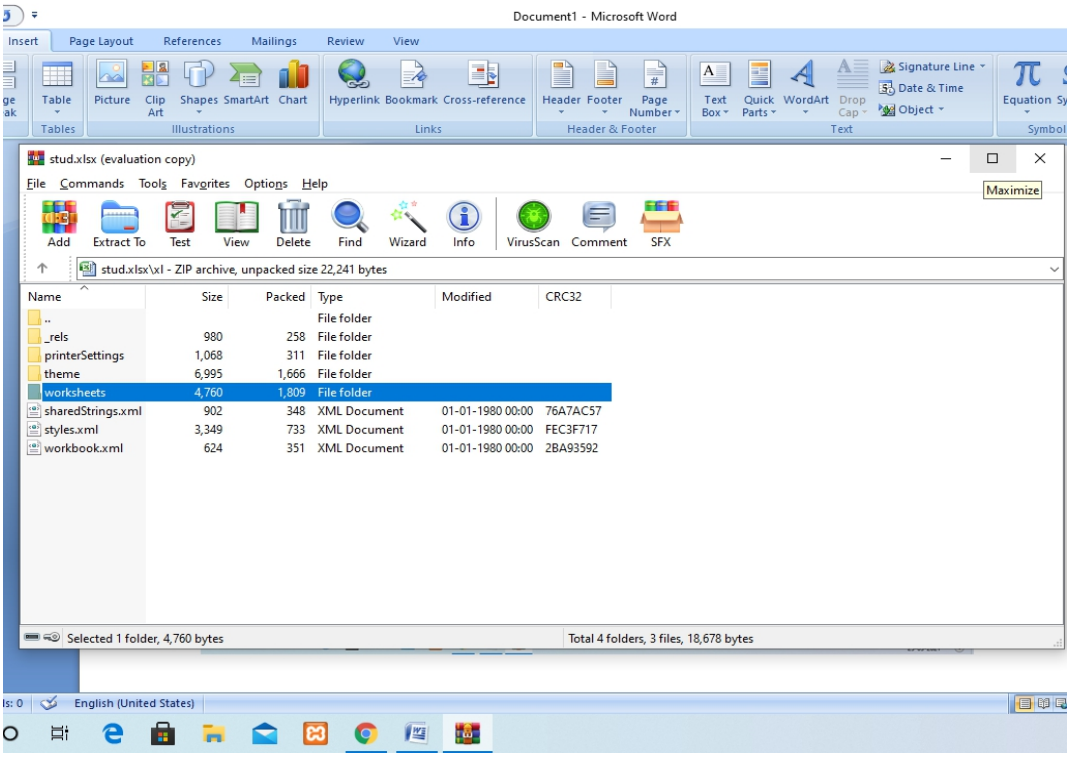
Step 10: Open the zip file by double click (or) right click and open



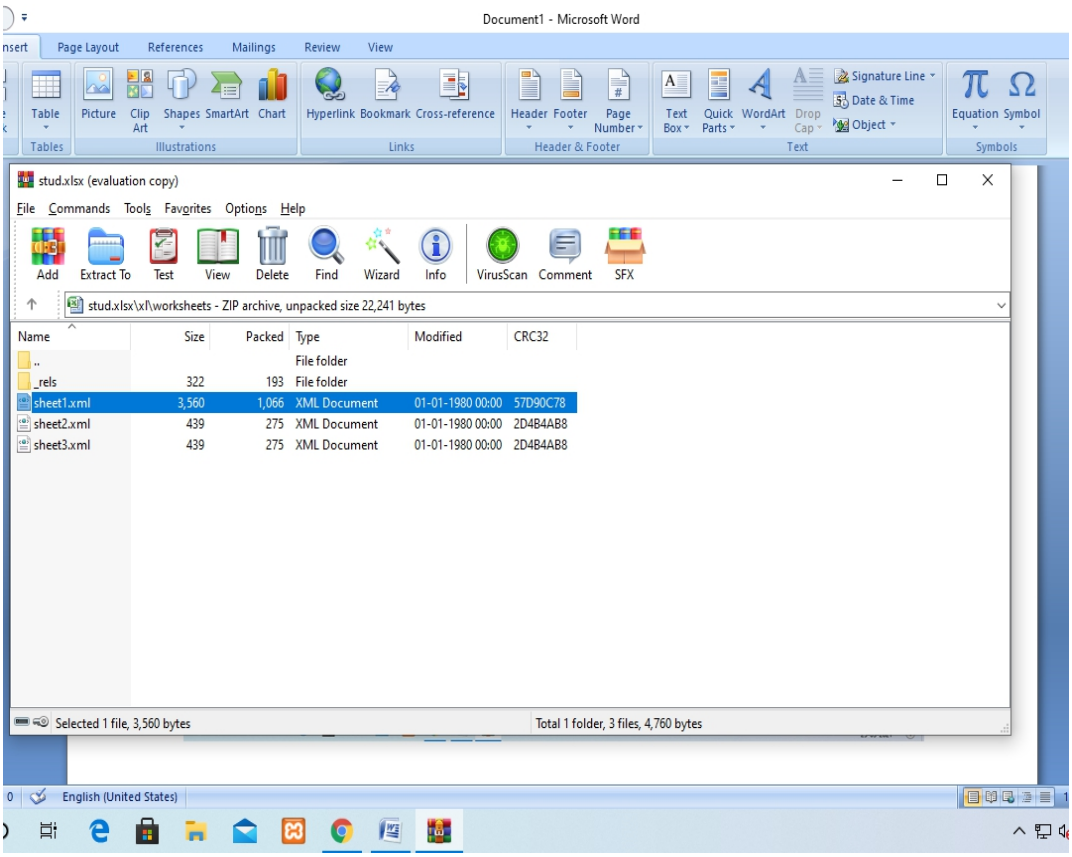
Step 11: Open the xs folder by double click (or) right click and open



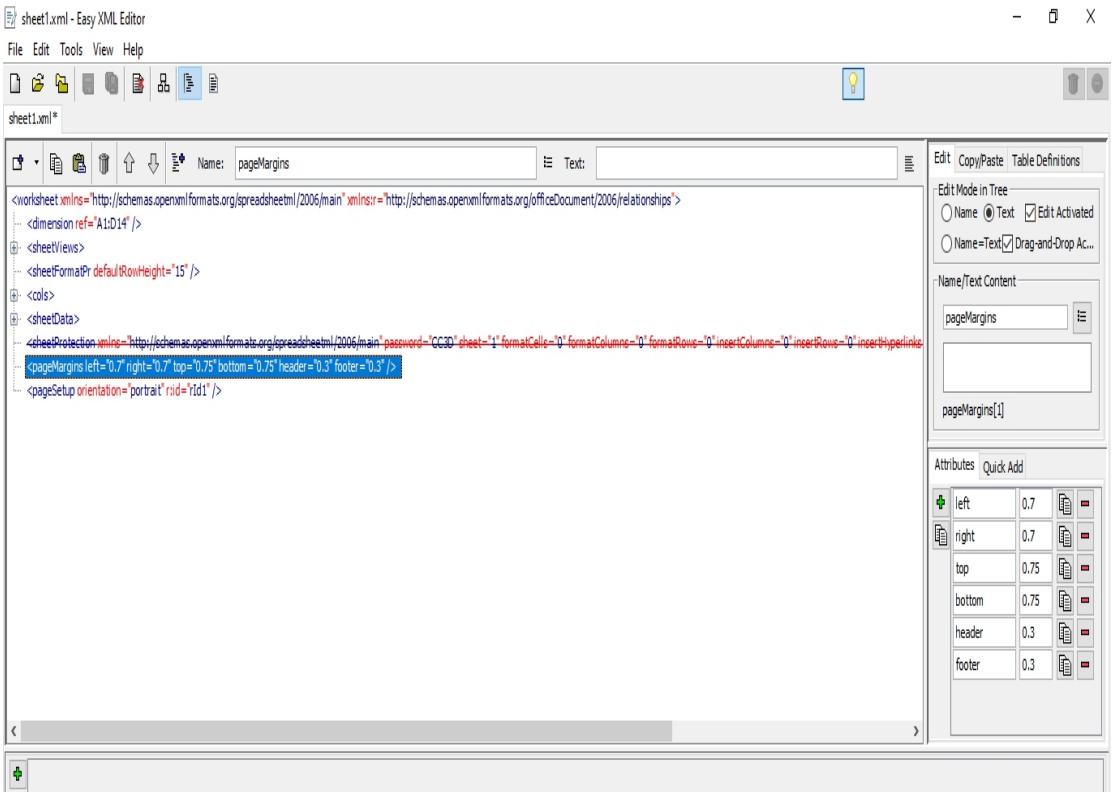
Step 12: Select the worksheet folder by double click (or) right click and open



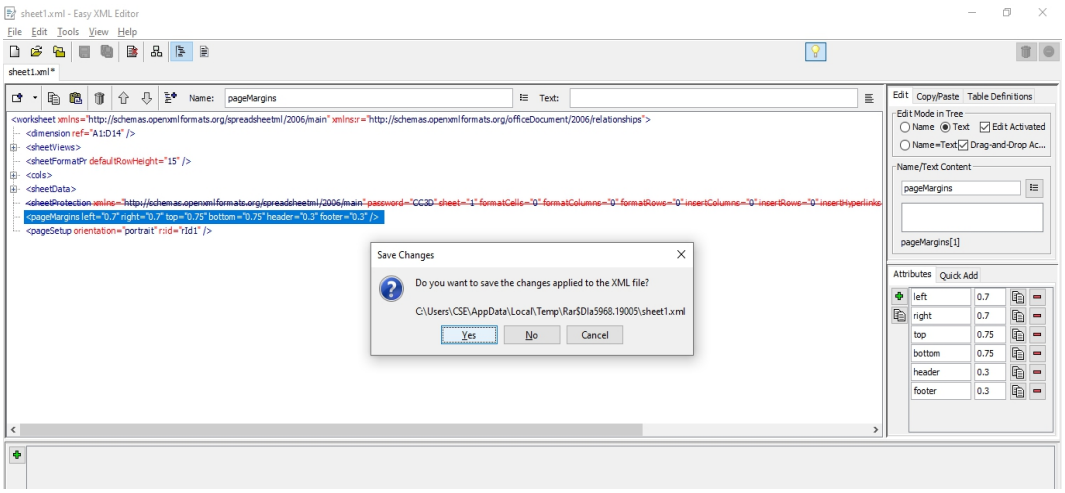
Step 13: Open the sheet1 were our official document get present



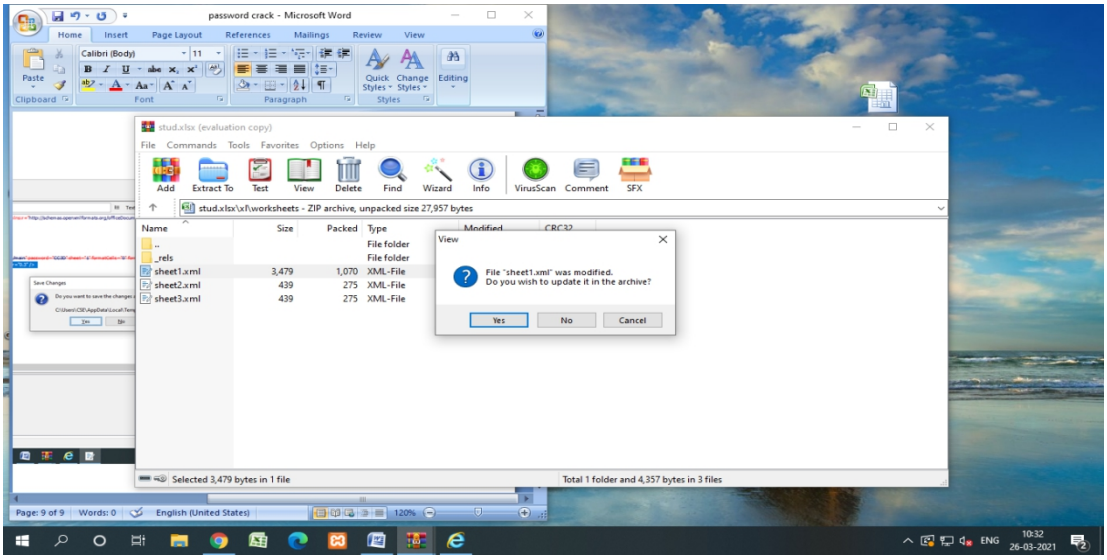
Step14: Select the password portion and delete it



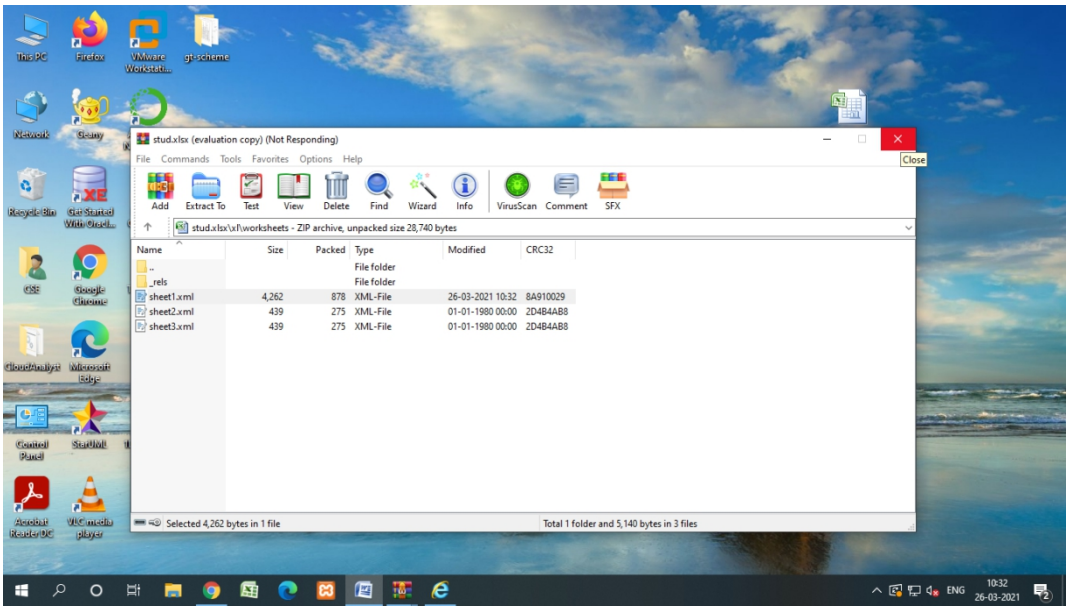
Step15: Finally save the document by selecting yes option



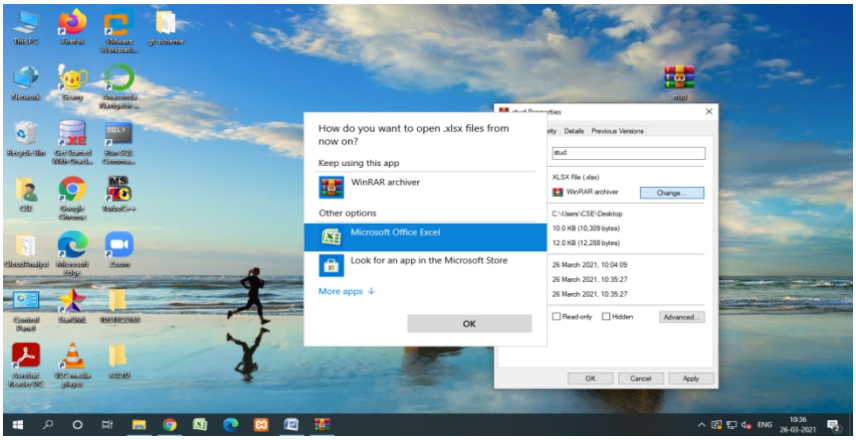
Step 16: Select yes to update the changes in the file



Step 17: Close the entire tab

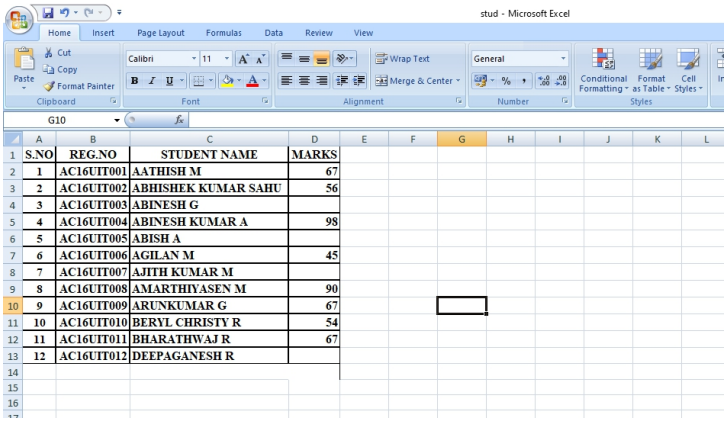


STEP 18: Again change the .zip format file to .xslx format



Step 19: The file again turned to .xslx format

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



stud - Microsoft Excel

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

RESULT:

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

EXPT.NO 4(A)	Analyze the problems and its preventive measure of Sniffing attack.	DATE:

AIM:

The main aim is to study the problems and prevention of sniffing attacks in detail.

PROCEDURE:

Sniffing refers to the use of software or hardware to watch data as it travels over the Internet. There are some legitimate uses for the process. It is then called network analysis and helps network administrators diagnose problems. In the hands of the wrong person, however, a sniffing program can collect passwords and read email. Sniffing is considered a passive security attack, according to TechiWarehouse.

What problems can result?

- Sniffing means a loss of privacy for those on a network. Along with the loss of privacy goes a loss of trust, which is necessary in many situations.
- Sniffing can compromise the privacy of passwords. An Ethernet sniffer can easily detect passwords.
- Sniffing can allow unauthorized persons access to financial information, including account numbers for banking and credit cards.
- Sniffing private and confidential information contained in email is very common. Having an email viewed by someone other than the intended recipient can cause problems ranging from embarrassment to a breach of national security.
- Sniffing can yield low-level protocol information. Anyone who is interested in attacking a network will then have the needed information.

Prevention:

- New data suggests that there is no way to detect when your computer has been sniffed. They also advise that while people can take measures to make sniffing difficult, it may be almost impossible to totally prevent being sniffed.
- Encryption helps. Replacing the hub with a switch may also add protection. Taking care when using public Wi-Fi may also help reduce exposure.

Consumer Fraud Reporting adds that you can help protect against spoofing by following these suggestions:

- Don’t click on an email link that requests personal information, even if it looks like a legitimate site.
- Be suspicious of anyone asking for personal information.

- Don’t send personal information or financial information through a Web site. If you’ve been caught in a moment of carelessness and provided information you should not have, such as passwords or personal identification, notify the companies you do business with right away to put a fraud alert on your account. Also contact Consumer Fraud Reporting, a free service that helps protect consumers against fraud.

RESULT:

The main aim is to study the problems and prevention of sniffing attacks in detail is studied successfully.

EXPT.NO 4(B)	Explore the Quickstego Tool for Hiding and Recovering the text and image based Information Using.	DATE

AIM:

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

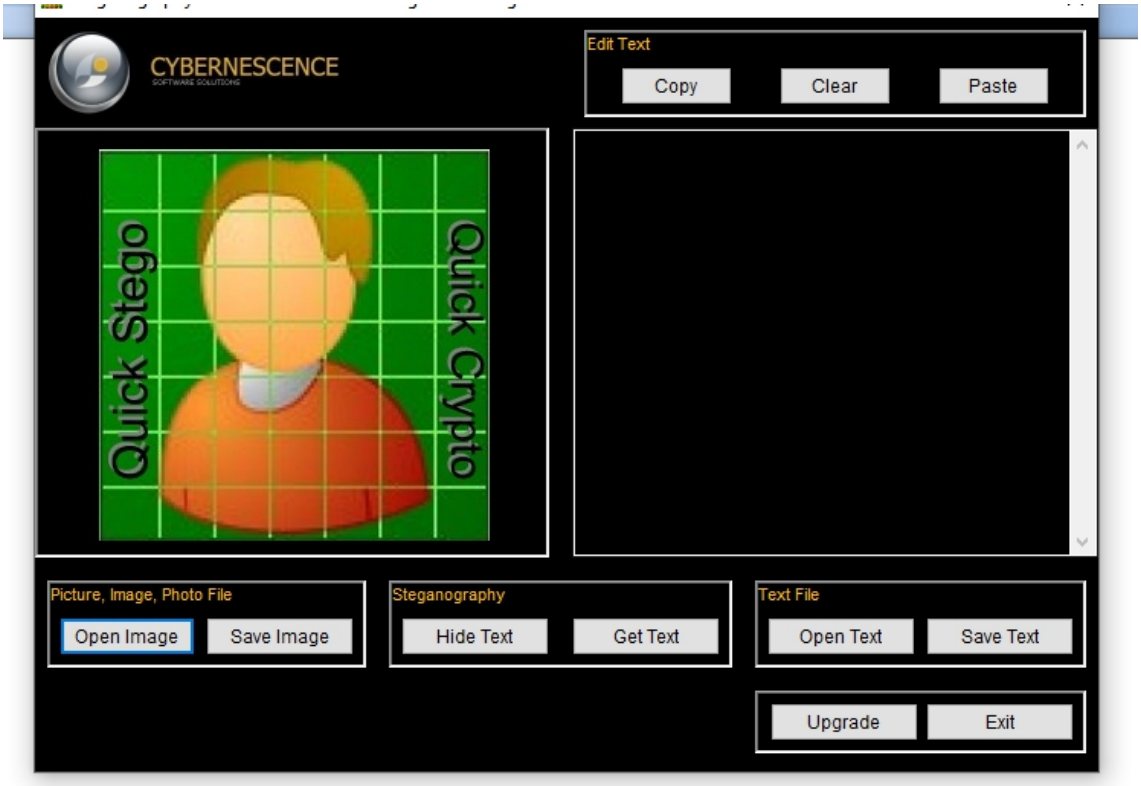
PROCEDURE:

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

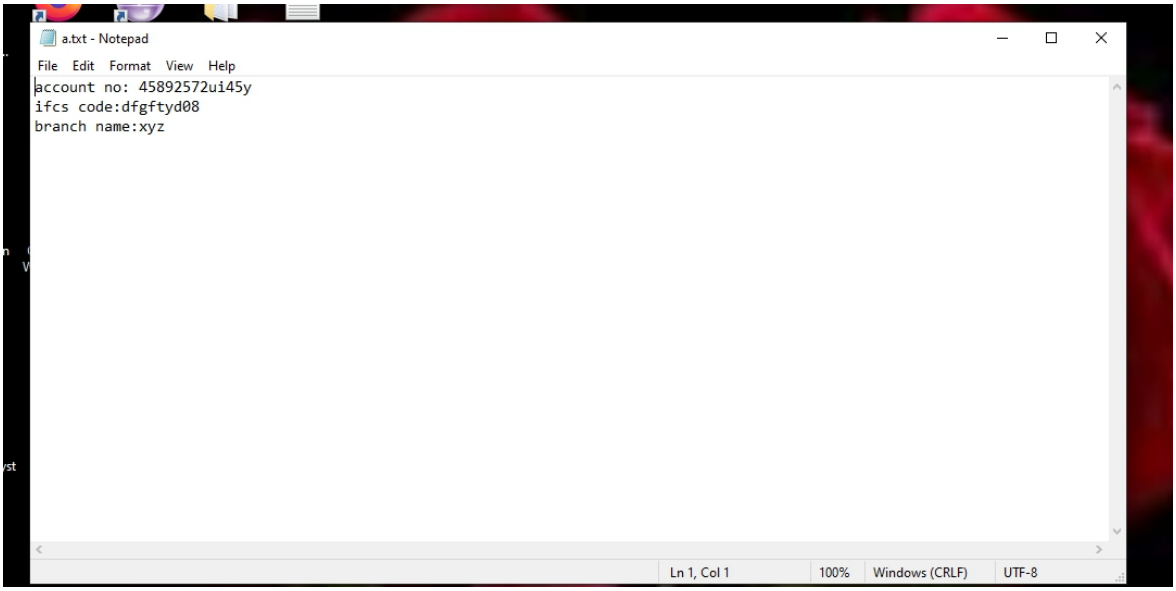
Step 1 : Download the QuickStego tool

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

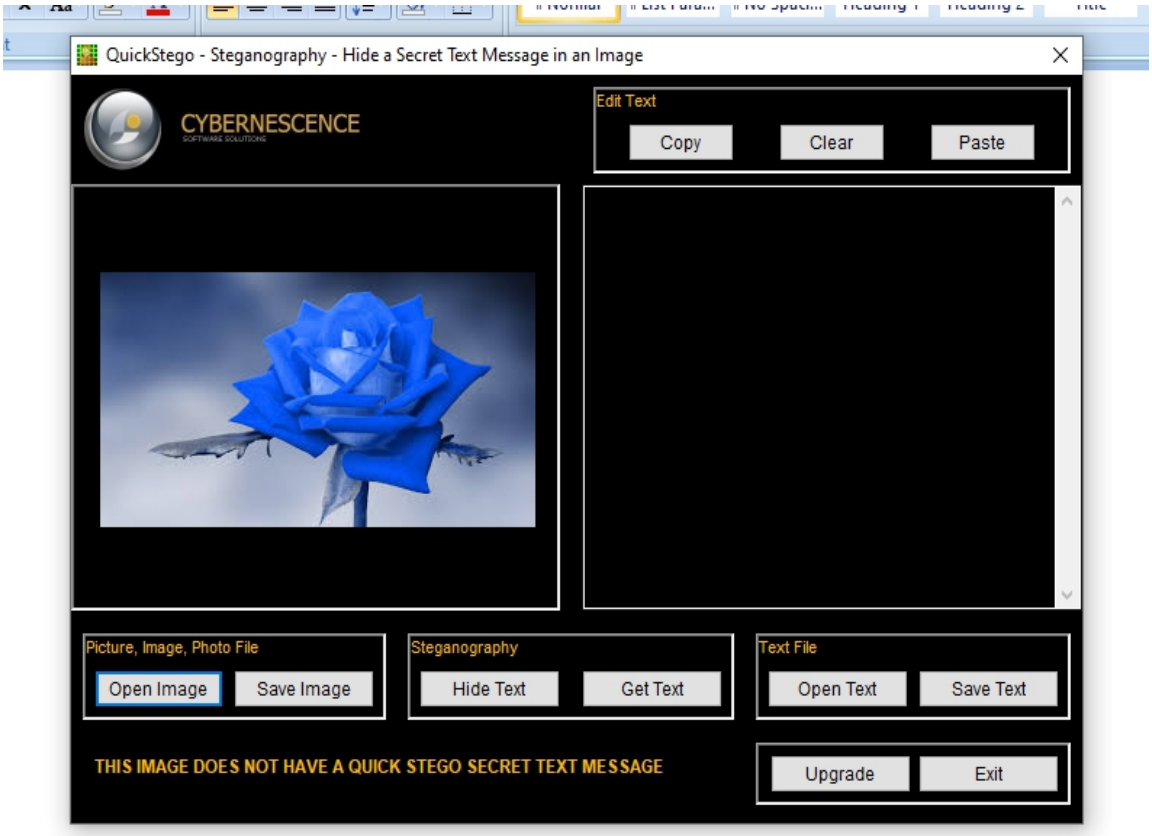
Step 3 : Open the QuickStego application



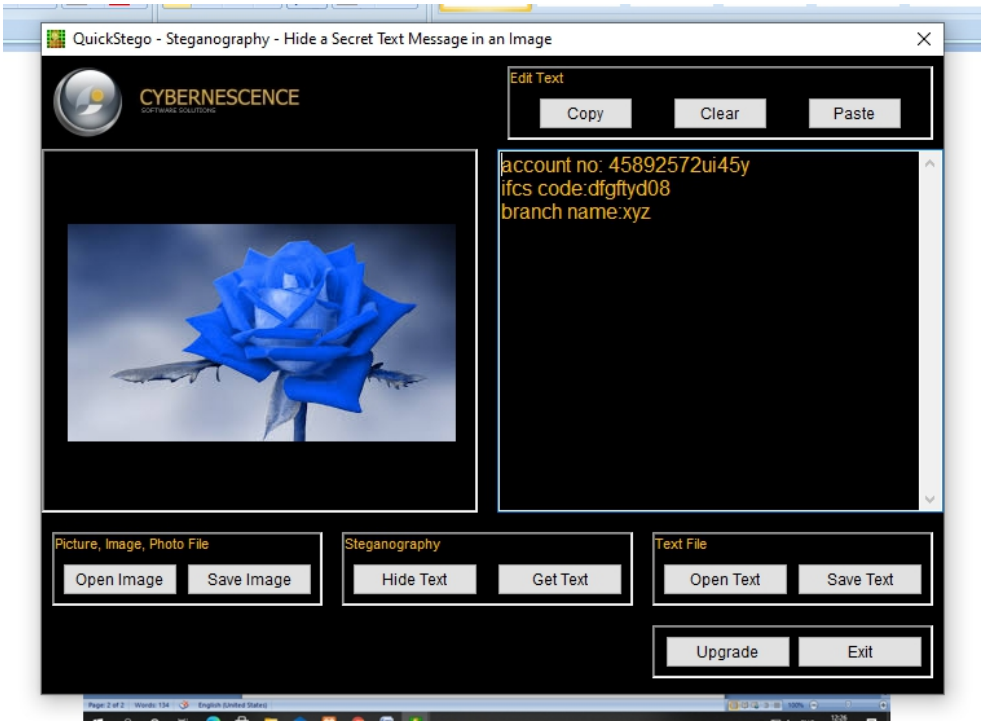
Step 4 : Create a text file or otherwise directly we can give the text data here we are creating a secrete text file with the extension .txt to upload in the image



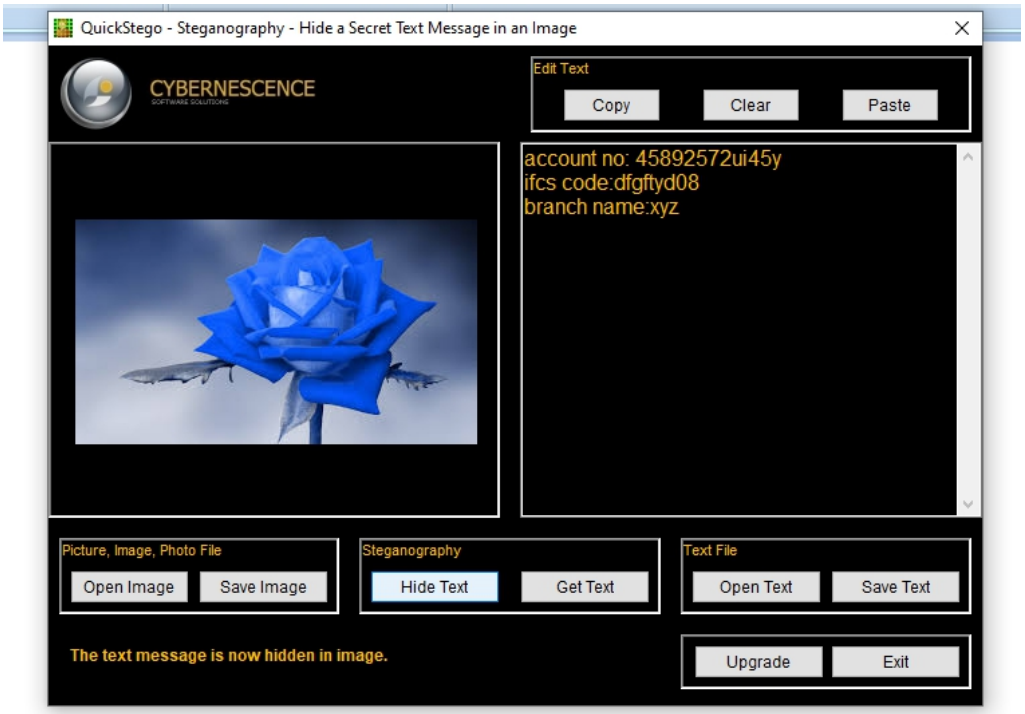
Step 5 : upload the image file to the QuickStego application



Step 6: Upload the text file to the QuickStego application



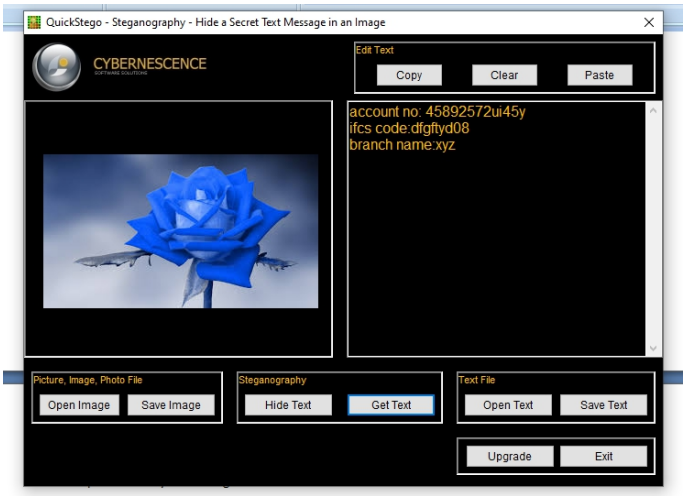
Step 7 : Click hide text to hide the text document to image



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

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

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



RESULT:

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

EXPT.NO 5(A)	STUDY OF CYBER FORENSIC TOOLS	DATE:

AIM:

The main aim is to Study the detail report of cyber forensic tools.

PROCEDURE:

Name	Platform	License	Version	Description
Autopsy	Windows, macOS, Linux	GPL	4.16	A digital forensics platform and GUI to The Sleuth Kit
AXIOM	Windows	proprietary	4.9	Full digital forensics suite by Magnet Forensics - Windows, MacOS, mobile and cloud supported in one platform
Belkasoft X	Windows	proprietary	1.0.6233	Digital forensic suite by Belkasoft, which supports computer and mobile forensics in a single tool
COFEE	Windows	proprietary	n/a	A suite of tools for Windows developed by Microsoft
Digital Forensics Framework	Unix-like/Windows	GPL	1.3	Framework and user interfaces dedicated to digital forensics
Elcomsoft Premium Forensic Bundle	Windows, macOS	proprietary	1435	Set of tools for encrypted systems & data decryption and password recovery
E3: Universal Software	Windows, macOS, Linux	GPL	2.6	E3: Universal develops by Paraben Corporation is and end-to-end DFIR solution that can work through ALL types of digital data: computers, email, internet data, smart phones, & IoT devices.
EnCase	Windows	proprietary	8.11	Digital forensics suite created by Guidance Software
Forensic Explorer	Windows	proprietary	5.4.2.1122	Digital forensics suite created by GetData

FTK	Windows	proprietary	7.3	Multi-purpose tool, FTK is a court-cited digital investigations platform built for speed, stability and ease of use.
IPED	Unix-like/Windows	GPL	3.17.2	Digital forensics tool created by the Brazilian Federal Police
ISEEK	Windows	proprietary	1	Hybrid-forensics tool running only in memory - designed for large networked environments
IsoBuster	Windows	proprietary	4.7	Essential light weight tool to inspect any type data carrier, supporting a wide range of file systems, with advanced export functionality.
Mobile Device Investigator	Windows,	proprietary	2.1	iOS and Android digital forensics and Smartphone triage tool by ADF_Solutions
Netherlands Forensic Institute / Xiraf/ HANSKEN	n/a	proprietary	n/a	Computer-forensic online service.
Open Computer Forensics Architecture	Linux	LGPL/GPL	2.3.0	Computer forensics framework for CF-Lab environment
OSForensics	Windows	proprietary	8	Multi-purpose forensic tool
PTK Forensics	LAMP	proprietary	2.0	GUI for The Sleuth Kit
SANS Investigative Forensics Toolkit - SIFT	Ubuntu		2.1	Multi-purpose forensic operating system
SPEKTOR Forensic Intelligence	Unix-like	proprietary	6.x	Easy to use, comprehensive forensic tool used worldwide by LE/Military/Agencies/Corporate - includes rapid imaging and fully automated analysis.

The Coroner's Toolkit	Unix-like	IBM Public License	1.19	A suite of programs for Unix analysis
The Sleuth Kit	Unix-like/Windows	IPL, CPL, GPL	4.1.2	A library of tools for both Unix and Windows
Windows To Go	n/a	proprietary	n/a	Bootable operating system
X-Ways Forensics	Windows	proprietary	n/a	Supports images and a bunch of volumes. And also memory and ram analysis

RESULT:

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

EXPT.NO 5(B)	Explore Compare It Tool to Compare of two files for Forensic Investigation.	DATE:

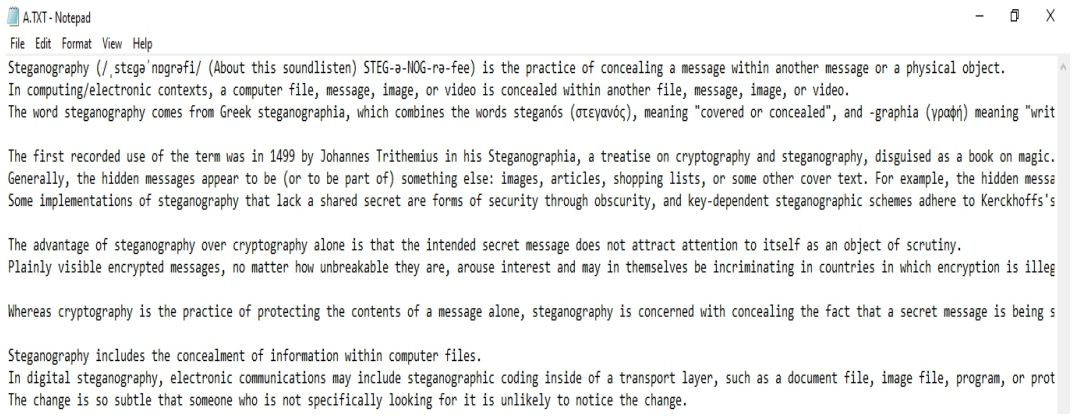
AIM:

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

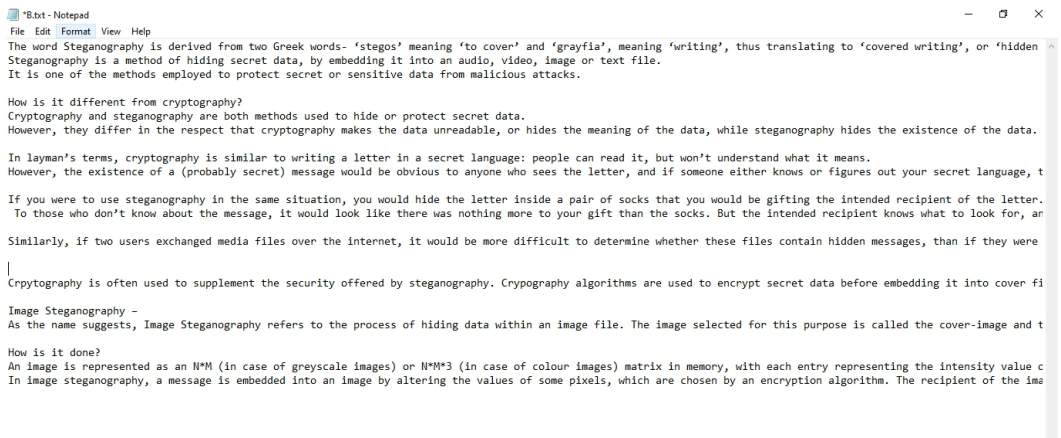
PROCEDURE:

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

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

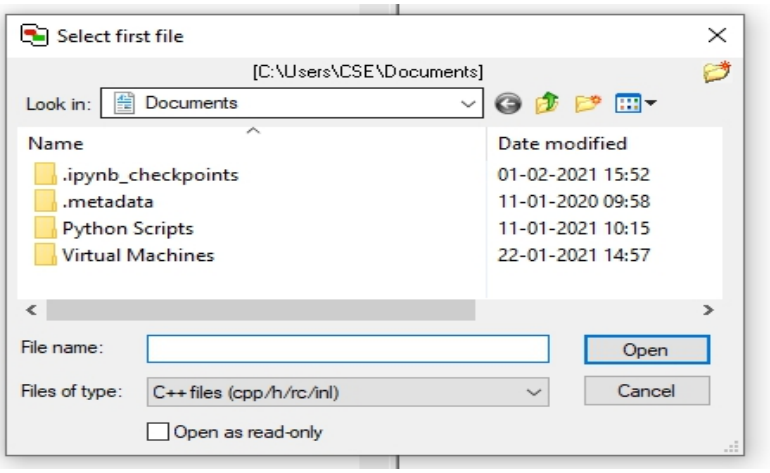


Step 2: create a second text file with the extension .txt

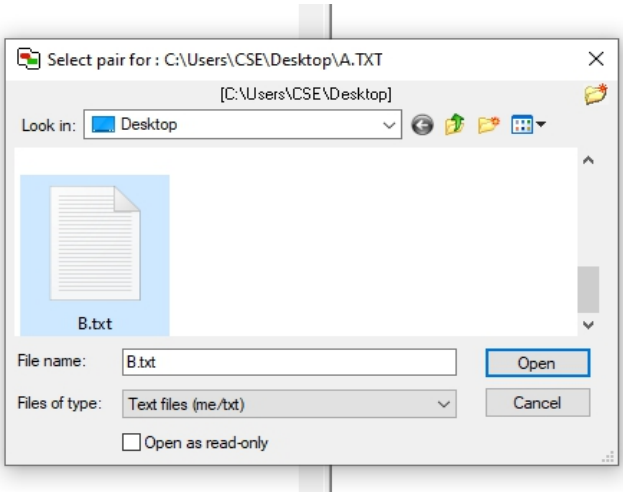


Step 4: Download the compare it tool install the Compare It from the Link given below. http://www.grigsoft.com/wincmp3.htm it is a 1.7 Mb Software package Click on Compare It Tool, It will show a window to select the files to be compared.

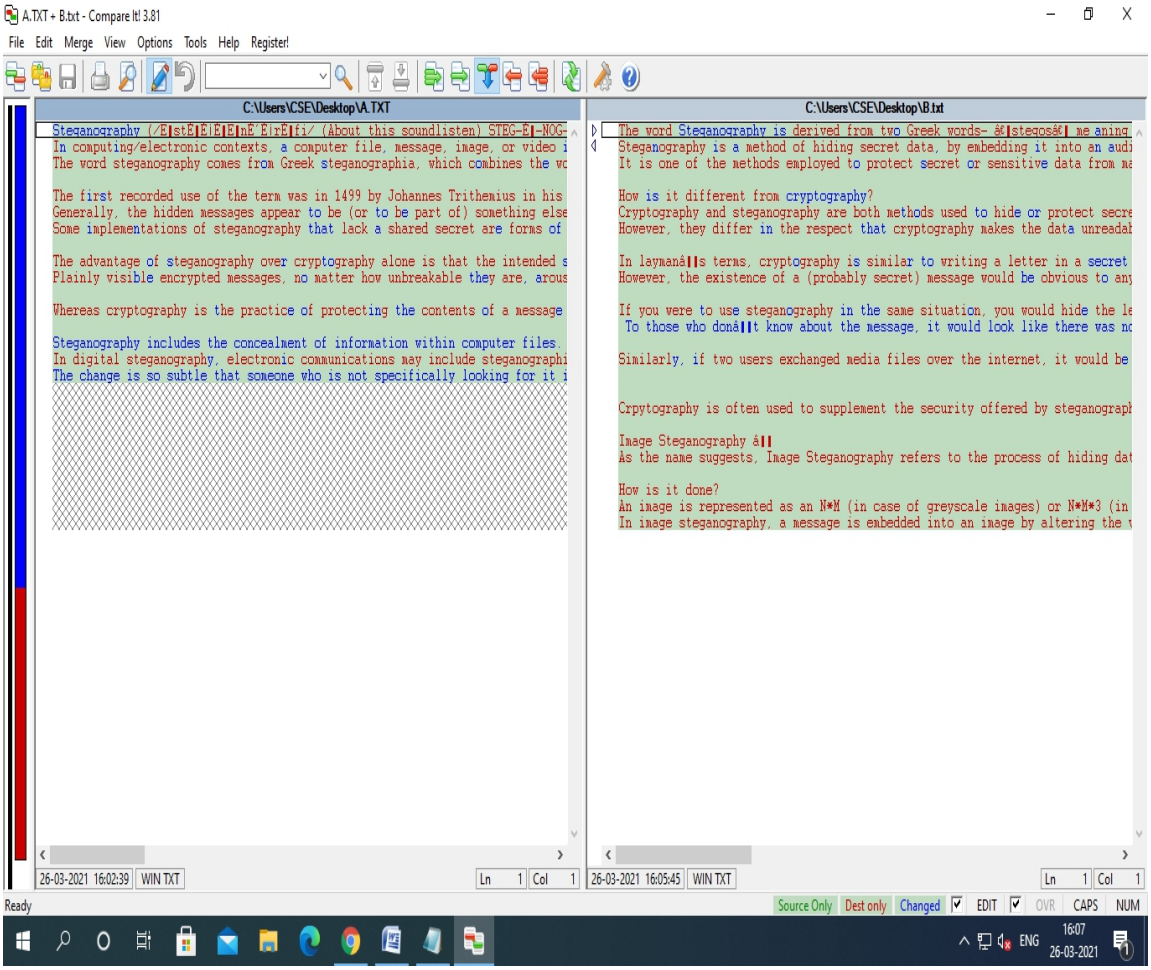
Step 5: Upload the first file to the compare it tool



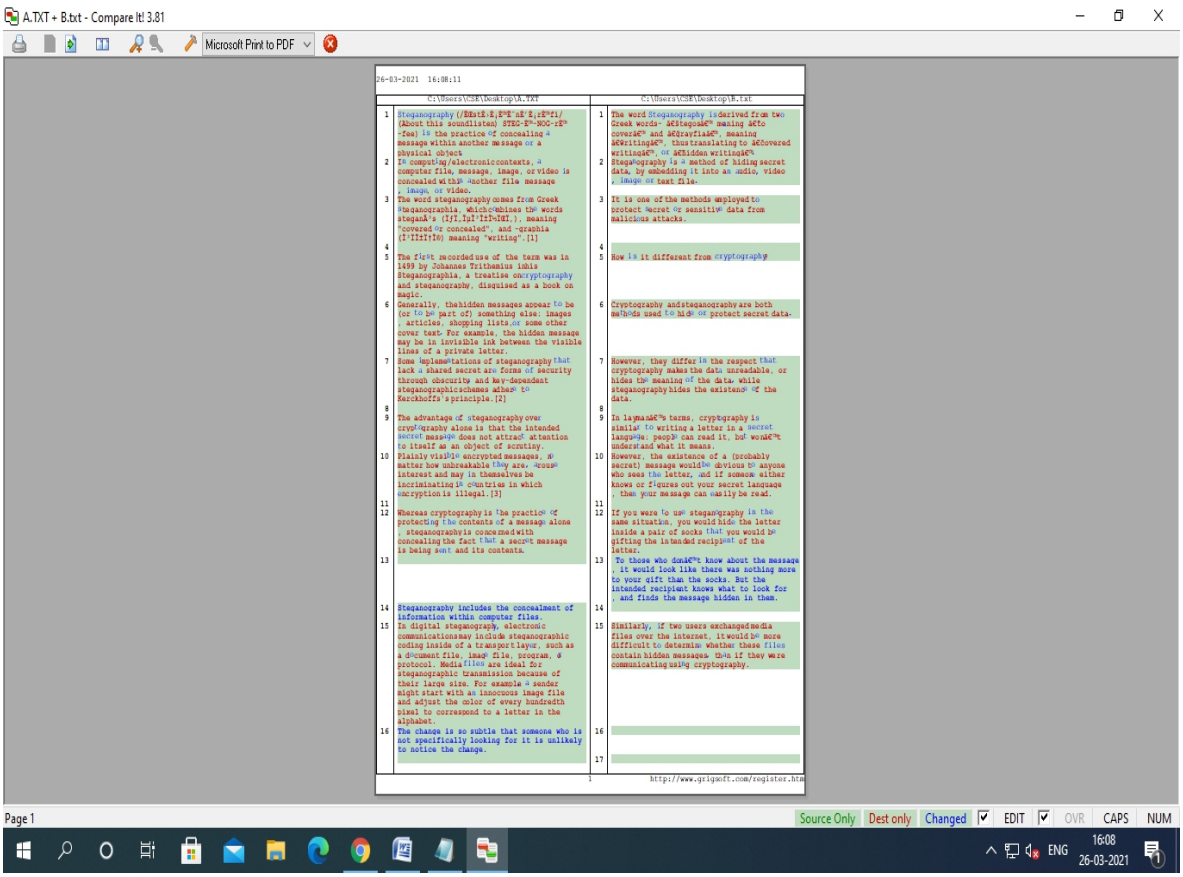
Step 6: upload the second file to the compare it tool



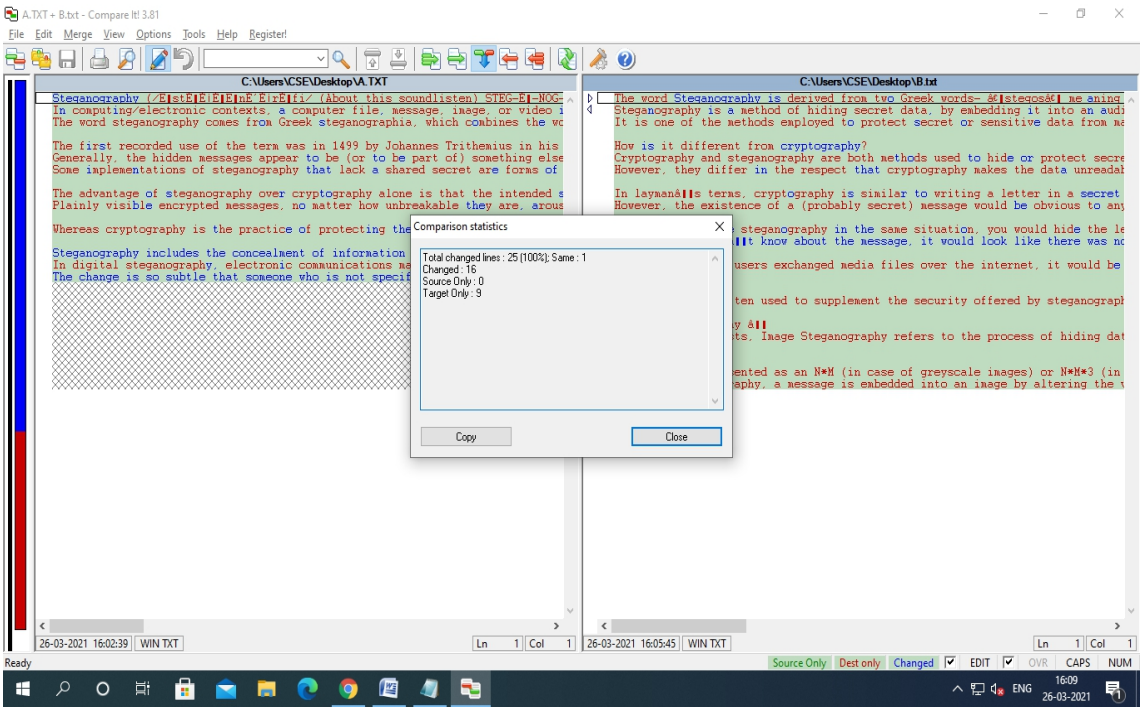
Step 7: Displays 2 files side by side, with colored differences sections to simplify analyzing. You can move changes between files with a single mouse click or keystroke



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



STEP 9: the comparison result is get display.



RESULT:

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

EXPT.NO 6(A)	Write the steps to Download a website using Website Copier tool (HTTrack)	DATE:

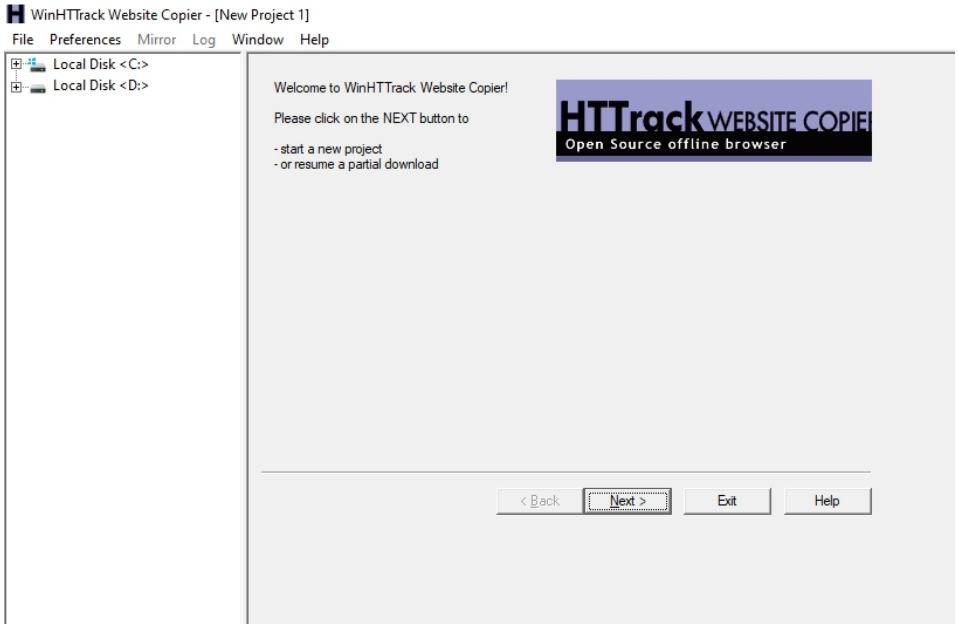
AIM:

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

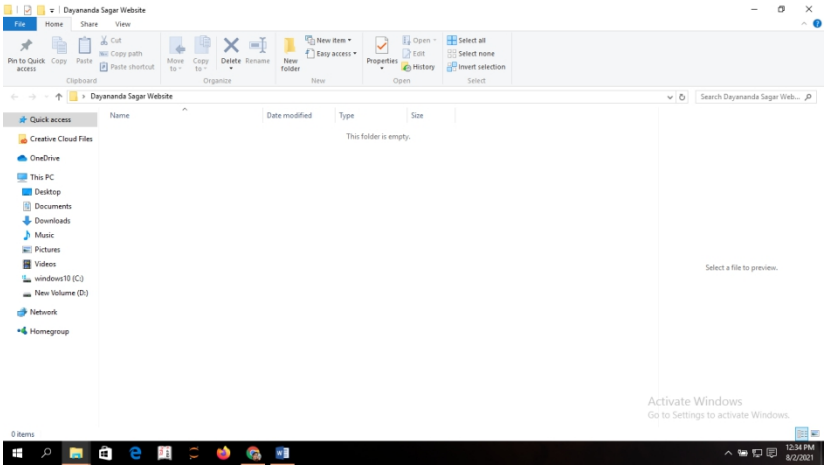
PROCEDURE:

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

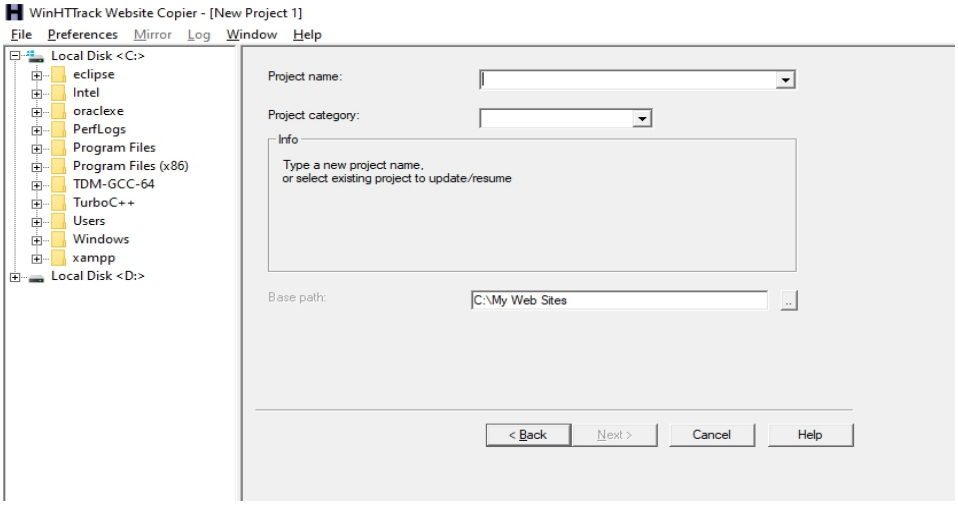
STEP 1: Install WinHTTrack



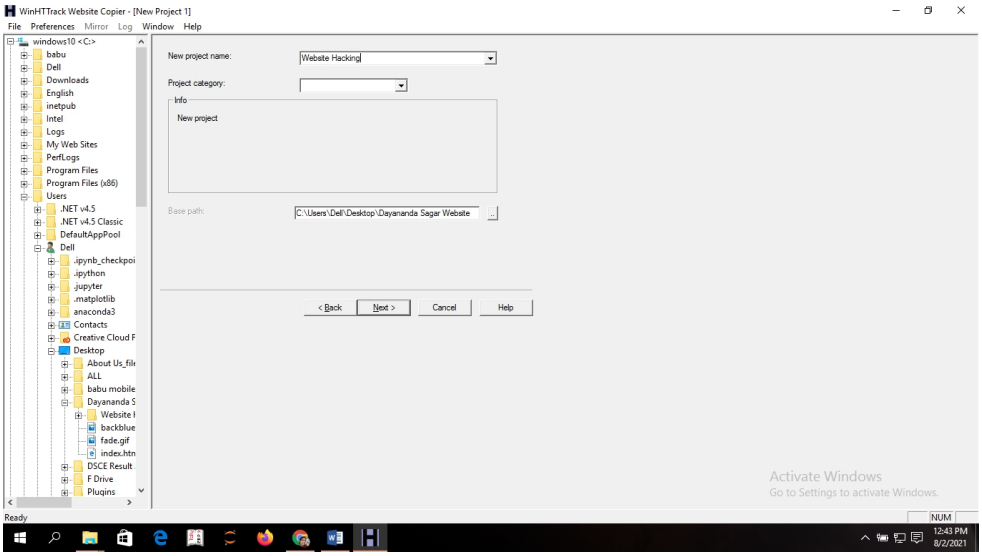
STEP 2: Create a folder on the Desktop and rename the folder
For Example: Folder name is “Dayananda Sagar Website”.
Open the folder “Dayananda Sagar Website”. The content of the folder is empty.



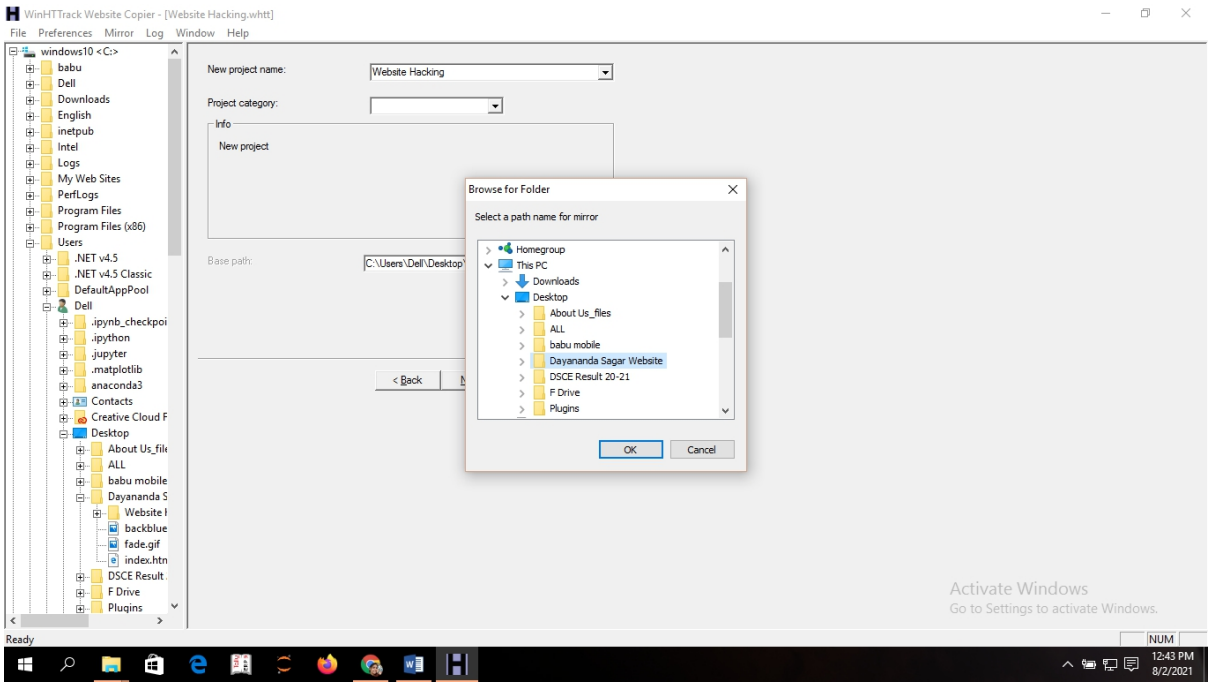
STEP 3: Select the new project from the file menu.



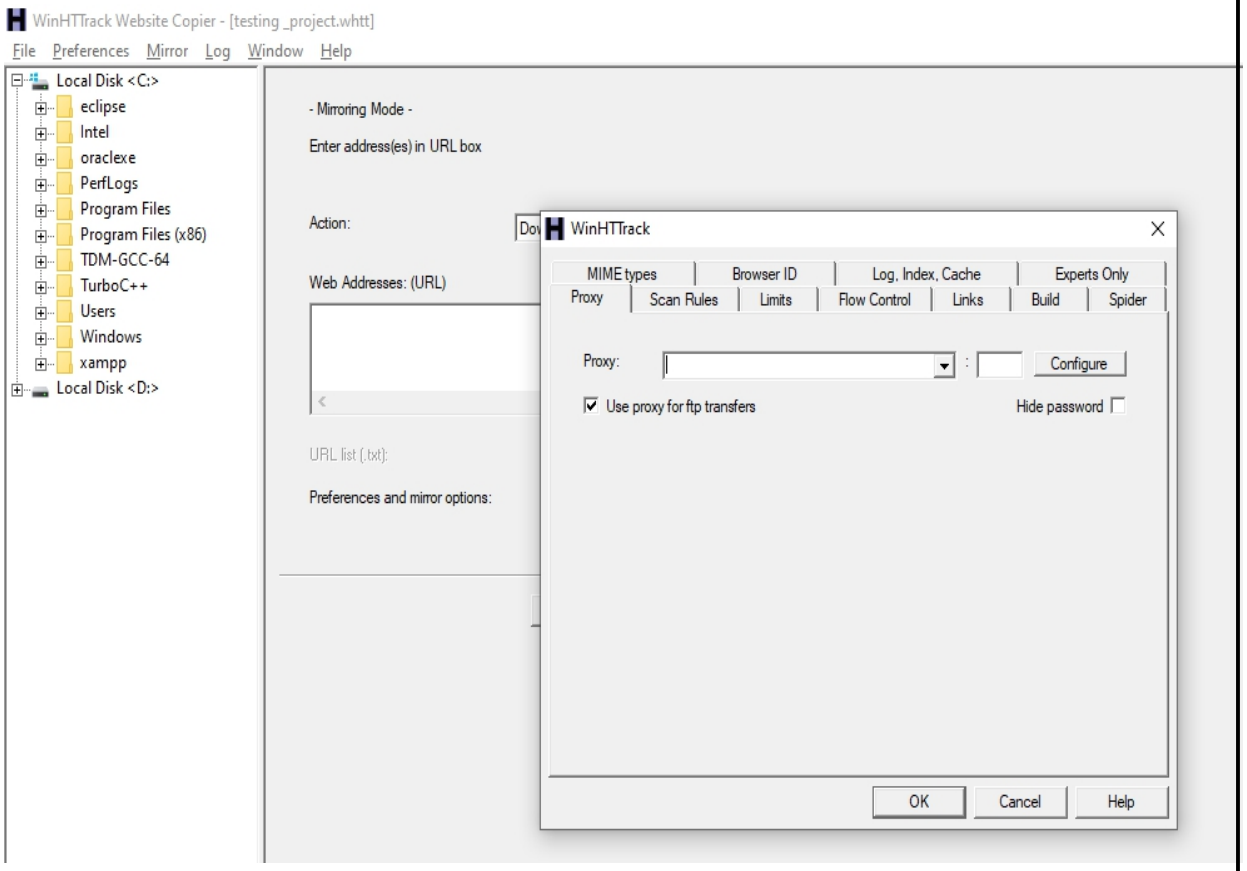
STEP 3: Enter the project name in new project field: **Example: Website hacking**



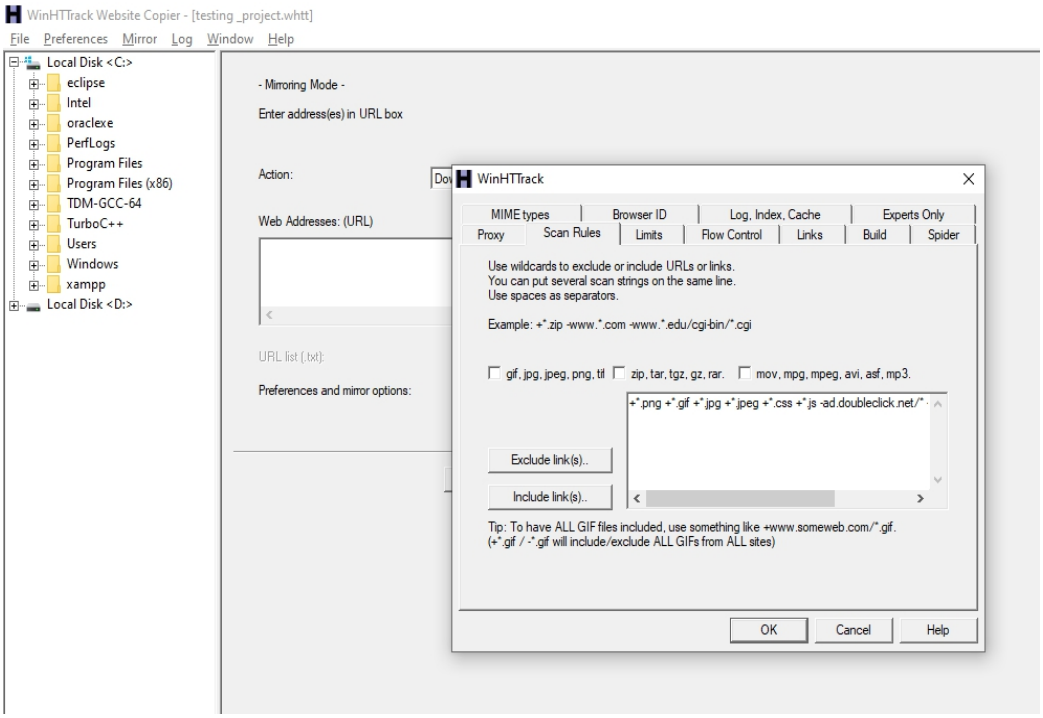
Step 4: Give the path where you need to download the files. In order to do this Click on Desktop and then click the folder “Dayananda Sagar Website”. Press OK



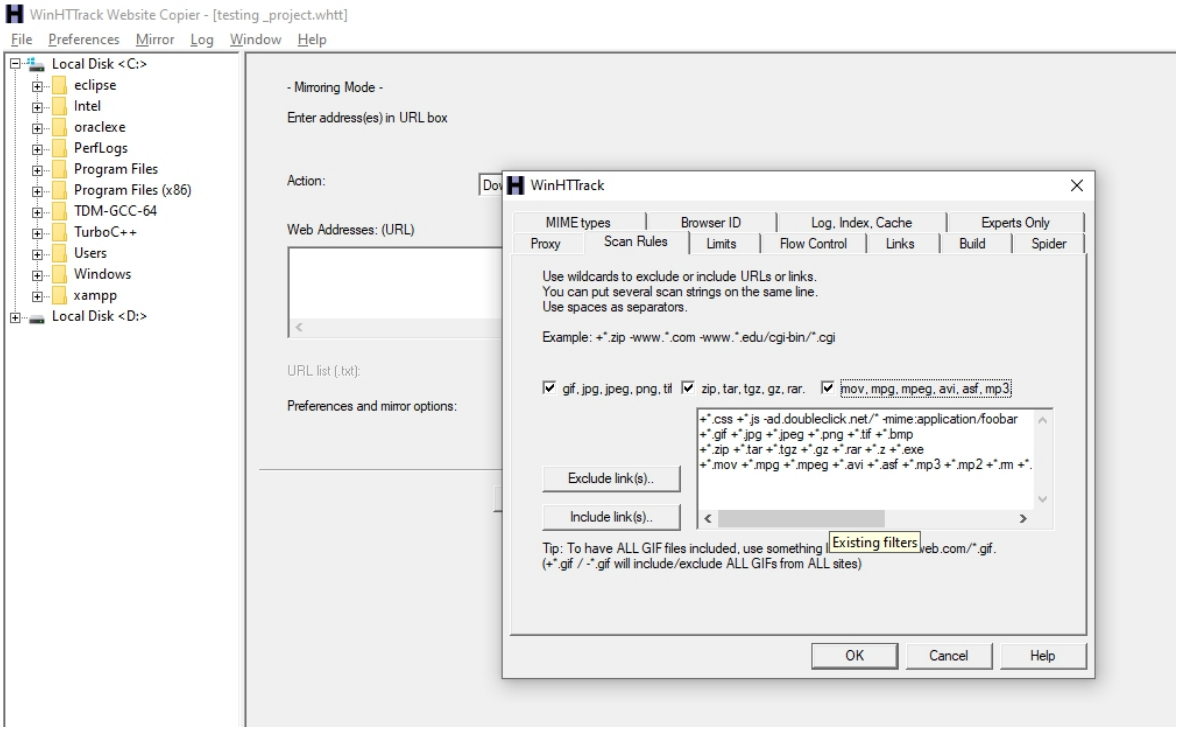
Step 5: WinHTTrack option window is opened select the scan rules



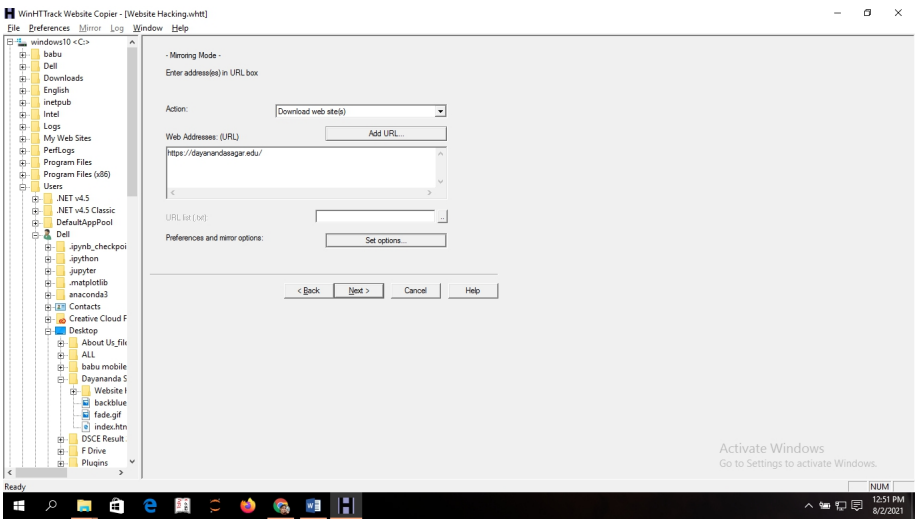
Step 6: Select all type of file to start the scan.



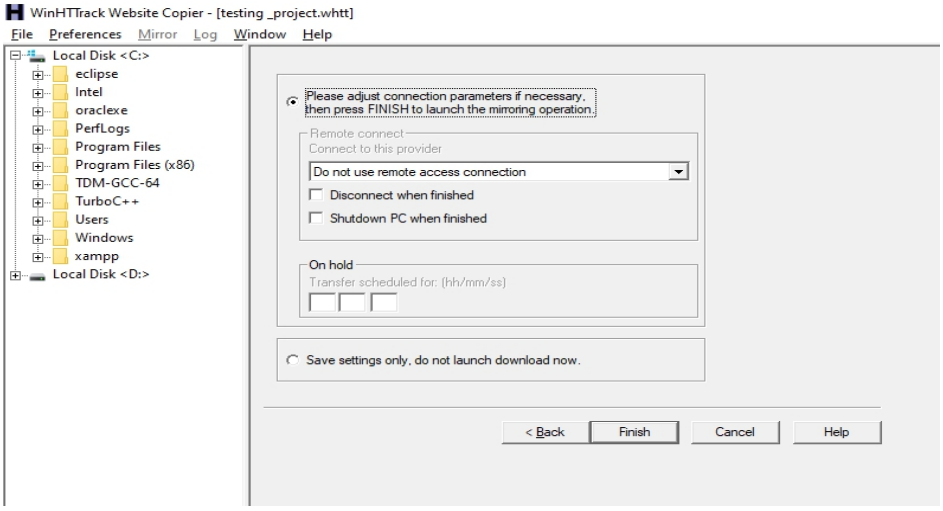
Step 7: Now all the extension is added for the scan.



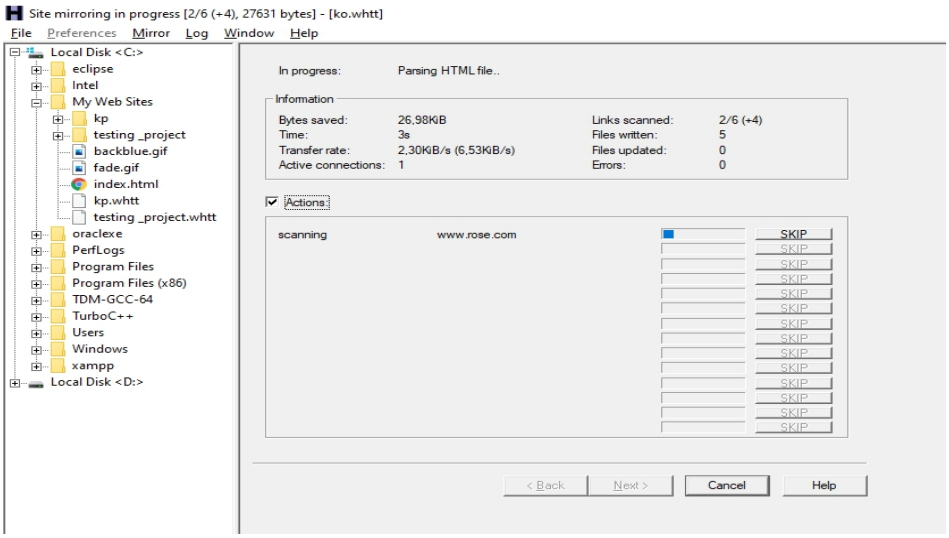
Step 8: Now type the URL address to scan



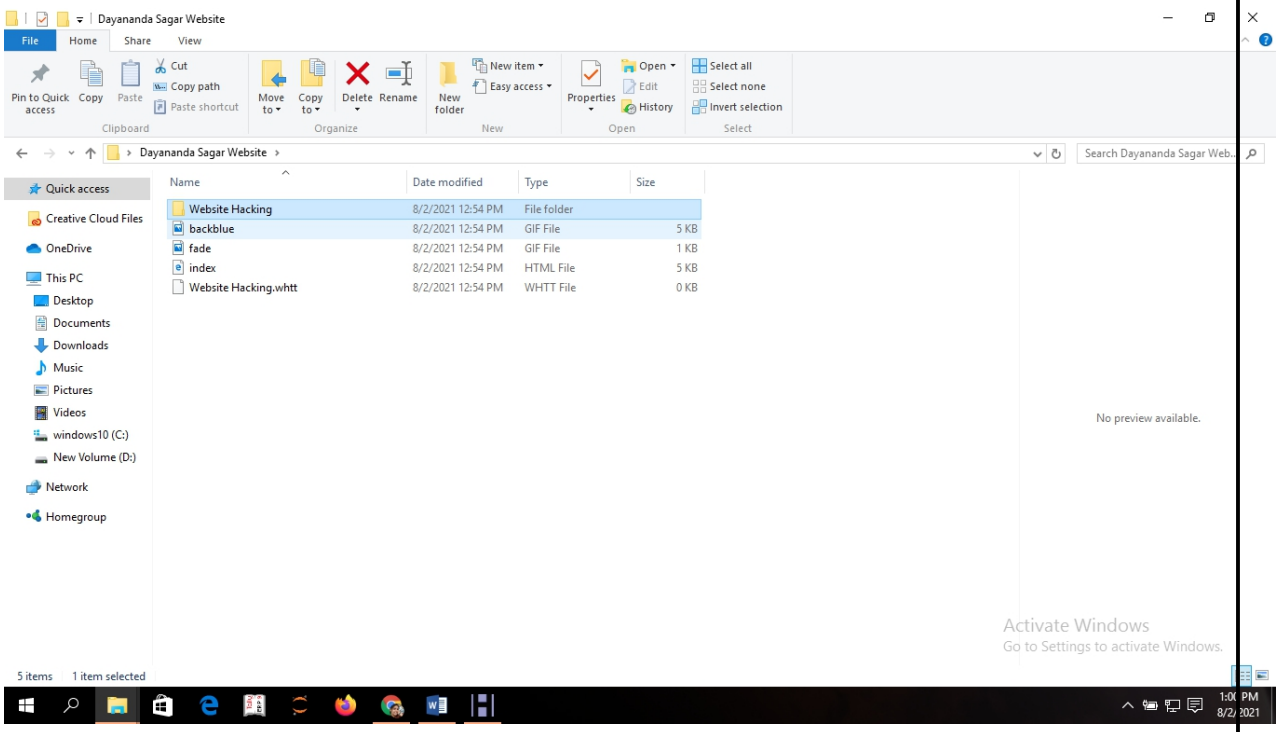
Step 9: Enable the connection adjustment if needed and click the finish button.



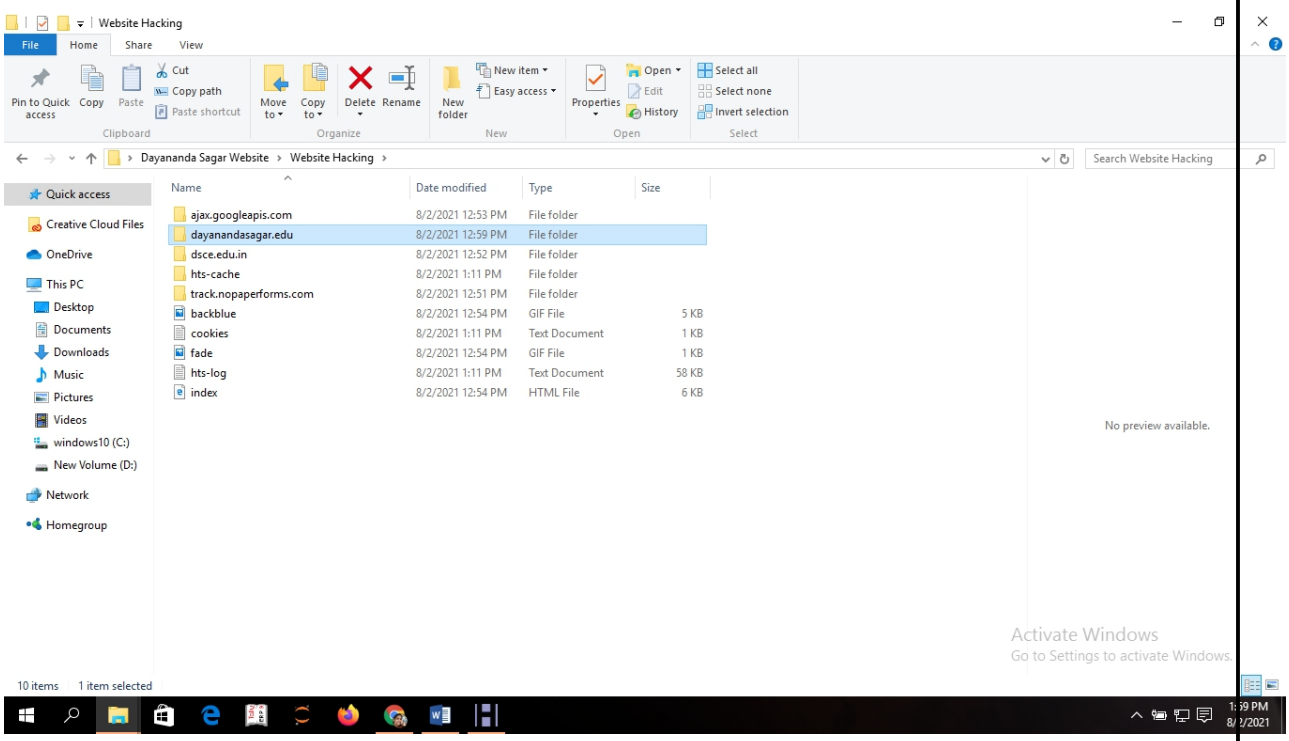
Step 10: mirroring process is get started



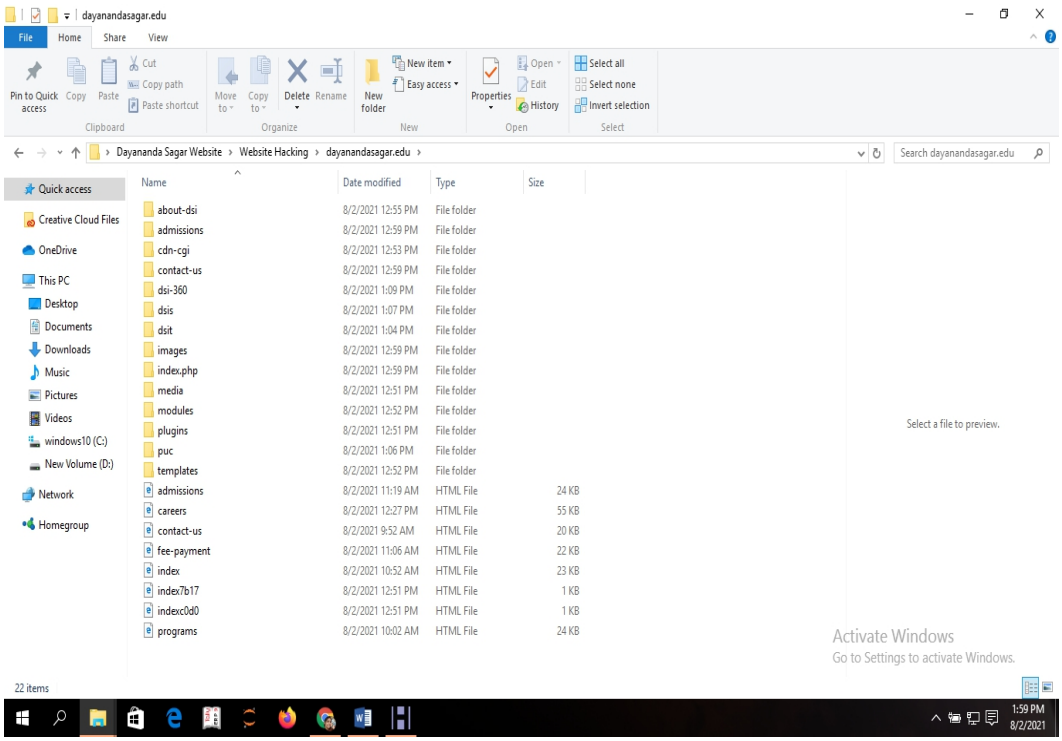
Step 11: The detail information about the URL will be fetched and saved in the folder “Dayananda Sagar Website”. You can now open the folder where you can see the the project name given as Website hacking as shown in Step 3.



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

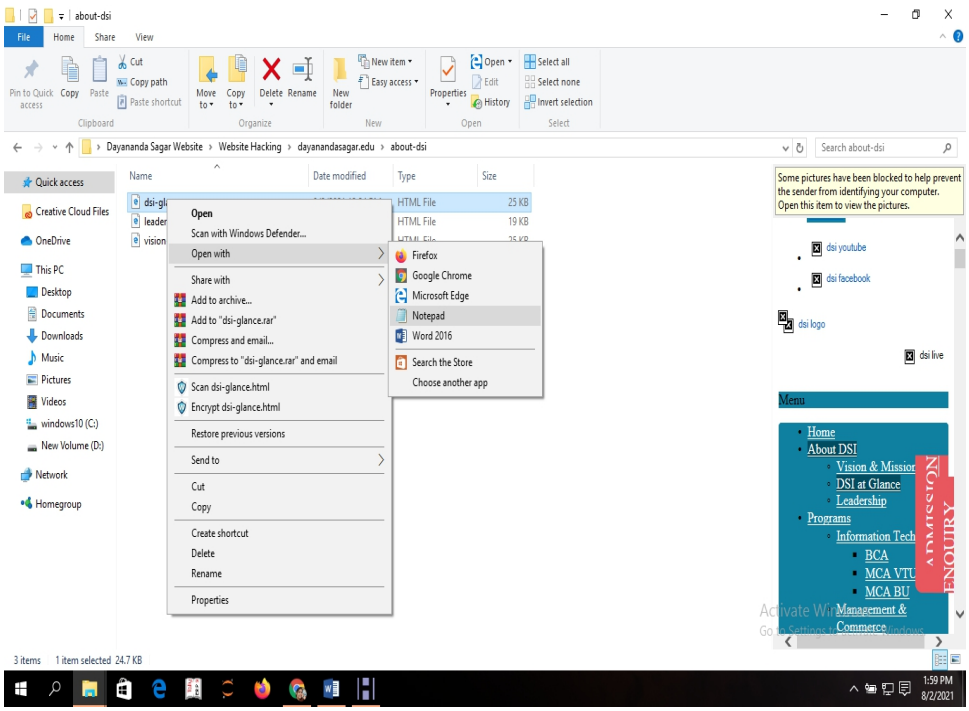


Step 13: Click on the file, dayanandasagar.edu. Now you can find all the files of the original page of the Website.

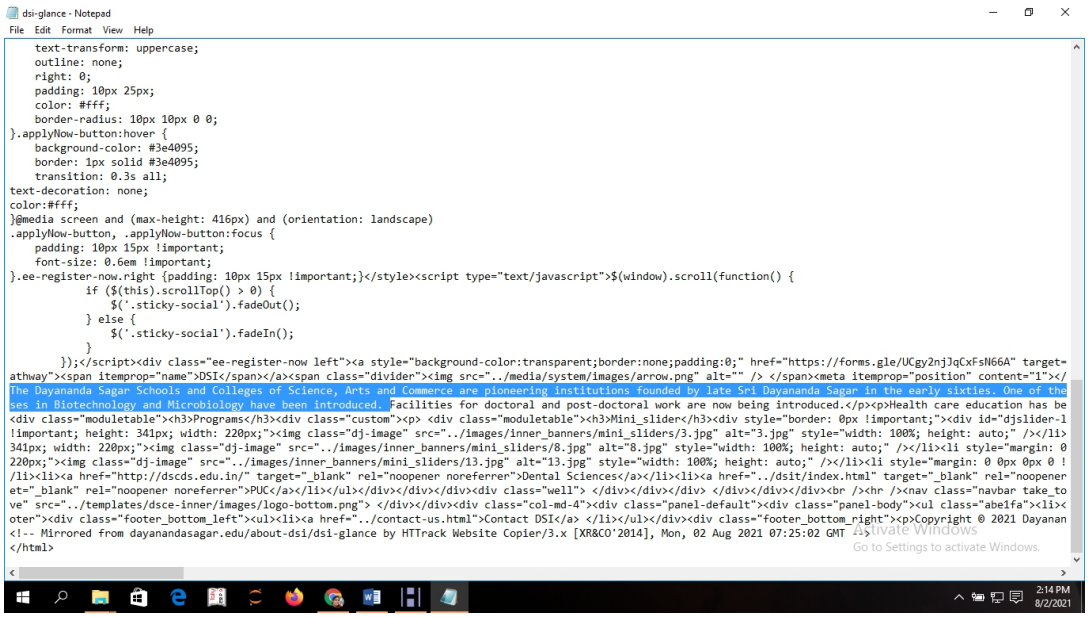


Step 14: Click on any file to alter the content : open with notepad.

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



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



RESULT:

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

EXPT.NO 6(B)	Explore the Snow Tool for hiding the information in Text File	DATE:

AIM:

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

PROCEDURE:

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

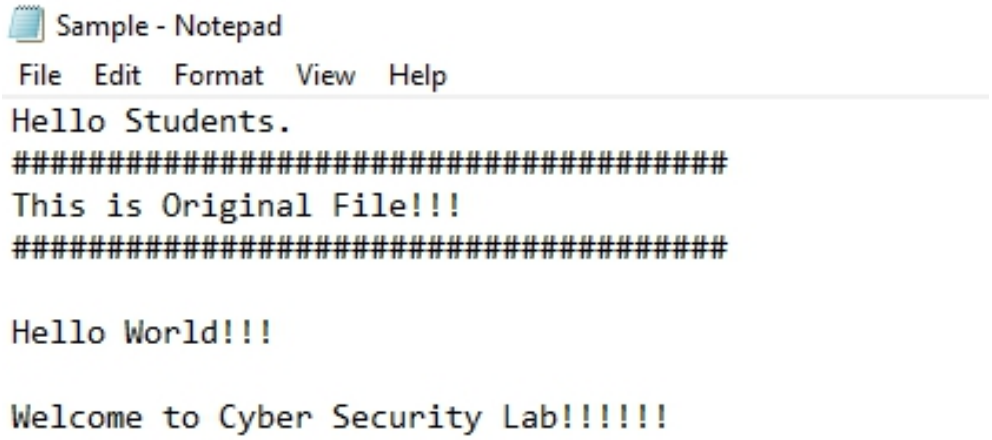


Figure: Text File

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

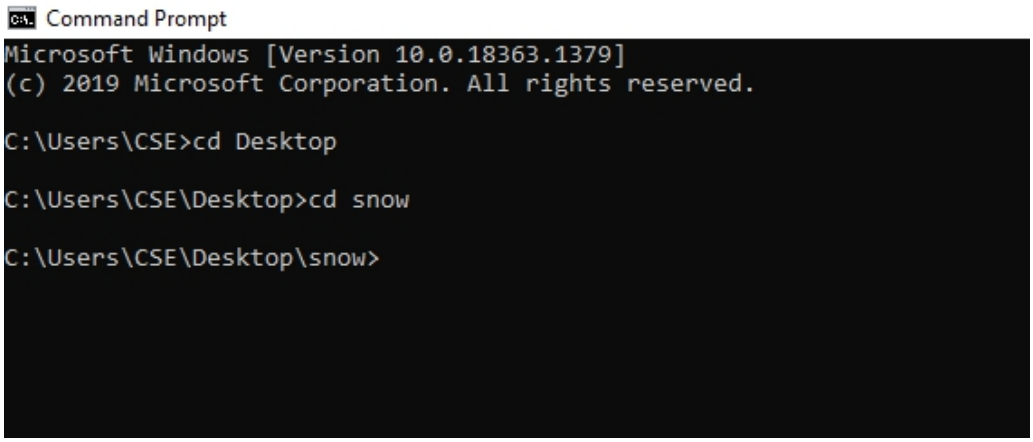


Figure: Changing the Directory

4) Type the Command:

snow -C -m “text to be hidden ” –p “password” <Source File><Destination File>

5) Example:

Snow -C -m “My Account number 1234567” –p “password123” Sample.txt Test.txt

The Source file is a Sample.txt file as shown above. Destination file will be created automatically and exact copy of source file containing hidden information.

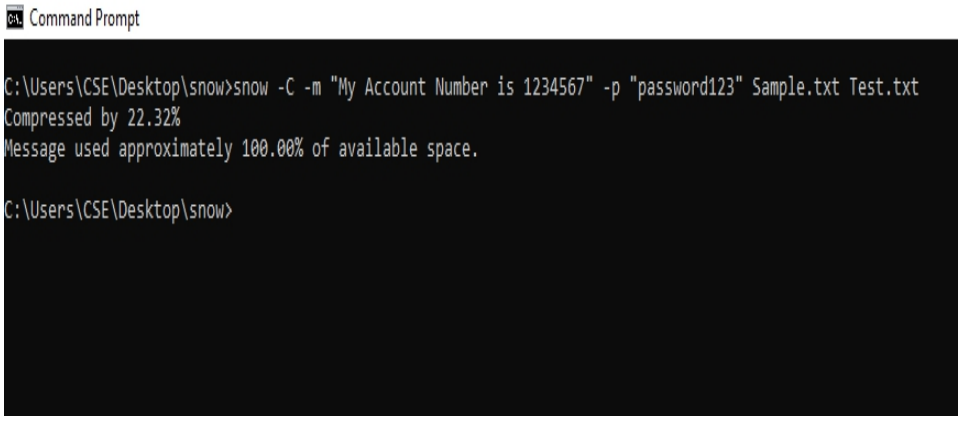


Figure: White Space Steganography using Snow Tool

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

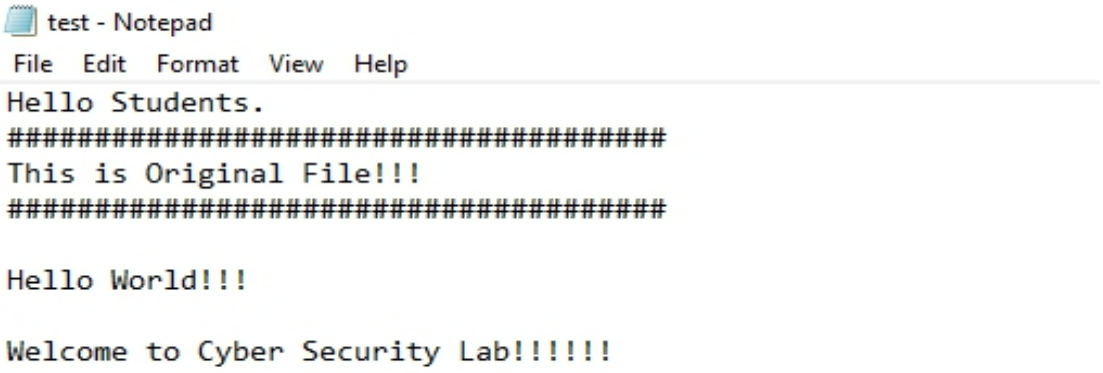


Figure: File Containing Hidden Encrypted Information

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

   On the Destination, the receiver can reveal information by using the command snow –C –p “password” <Destination File>

   snow –C –p “password123” test.txt

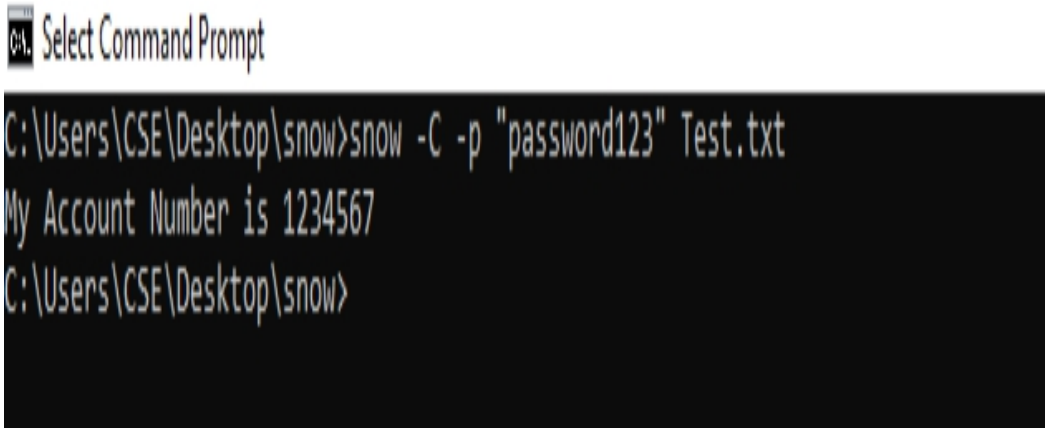


Figure: Decrypting File

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

RESULT:

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

EXPT.NO 7(A)	Illustrate the defamation and repairment solution caused by Virus and Trojans	DATE:

AIM:

The main aim is to study of different attack caused virus and Trojans.

PROCEDURE:

Virus:

- The most potent and vulnerable threat of computer users is virus attacks.
- Virus attacks hampers important work involved with data and documents.
- It is imperative for every computer user to be aware about the software and programs that can help to protect the personal computers from attacks. One must take every possible measure in order to keep the computer systems free from virus attacks.

The top sources of virus attacks are highlighted below:

- Downloadable Programs
- Cracked Software
- Email Attachments
- Internet
- Booting From CD

Trojans:

- Trojan horse attacks pose one of the most serious threats to computer security. If you were referred here, you may have not only been attacked but may also be attacking others unknowingly.
- According to legend, the Greeks won the Trojan war by hiding in a huge, hollow wooden horse to sneak into the fortified city of Troy.
- In today's computer world, a Trojan horse is defined as a "malicious, security-breaking program that is disguised as something benign".
- For example, you download what appears to be a movie or music file, but when you click on it, you unleash a dangerous program that erases your disk, sends your credit card numbers and passwords to a stranger, or lets that stranger hijack your computer to commit illegal denial of service attacks.

Repairing the Damage

1. Anti-Virus Software: Compared to traditional viruses, today's trojans evolve much quicker and come in many seemingly innocuous forms, so anti-virus software is always going to be playing catch up. Also, if they fail to find every trojan, anti-virus software can

give you a false sense of security, such that you go about your business not realizing that you are still dangerously compromised. There are many products to choose from, but the following are generally effective: AVP, PC-cillin, and McAfee Virus Scan. For a more complete review of all major anti-virus programs, including specific configuration suggestions for each, see the Hack Fix Project's anti-virus software page .

2. Anti-Trojan Programs:

These programs are the most effective against trojan horse attacks, because they specialize in trojans instead of general viruses. A popular choice is The Cleaner, To use it effectively when you are done, make sure you've updated Windows with all security patches, then change all your passwords because they may have been seen by every "hacker" in the world.

RESULT:

The main aim is to study of different attack caused virus and Trojans is completed successfully.

EXPT.NO 7(B)	Write a program to illustrate Buffer overflow attack	DATE:

AIM:

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

PROCEDURE:

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

```
#include <stdio.h>
#include <string.h>

int main(void)

{

   char buff[15];

   int pass = 0;

   printf("\n Enter the password : \n");

   gets(buff);

   if(strcmp(buff, "thegeekstuff"))

   {

      printf ("\n Wrong Password \n");

   }

   else

   {

      printf ("\n Correct Password \n");

      pass = 1;

   }

   if(pass)

   {

     /* Now Give root or admin rights to user*/

      printf ("\n Root privileges given to the user \n");

   }
```

```
    return 0;
}
```

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

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

OUTPUT

RUN1

Enter the password :

thegeekstuff

Correct Password

Root privileges given to the user

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

Here is an example :

RUN 2

Enter the password :

hhhhhhhhhhhhhhhhhhhh

Wrong Password

Root privileges given to the user

RESULT:

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

EXPT.NO 8(A)	Analyze the Security Issues and Threats in E-Mail Application	DATE:

AIM:

The main aim is to analyze the security issues and threats in e-mail application in detail.

PROCEDURE:

Security Issues and vulnerability in Email System:

E-mail is one of the main modes of communication today but in the following section it can be seen how insecure it is. The importance of email is for corporate and private communication can be estimated by the summary presented by Radicati Group's report titled "E-Mail Market, 2012- 2016" that the world wide each day total emails sent in 2012 was 144.8 billion, which is increased steadily with each passing year and in 2016 approximately 192.2 billion emails will sent each day. The report also states that corporate webmail clients grow from 629 million in 2012 to over one billion by the end of 2016.

Threats in Email Communication:

Eavesdropping: E-mail messages pass through networks which are part of big picture i.e. Internet with a lot of people on it. So it is very easy for someone to track or capture your message and read it.

Identity Theft:

Means someone pretend to be you on the network. It may be possible if not proper security protocols are followed that someone may steal or capture your username/password and used to read your email messages. Further also send email messages from your account without your knowledge.

Unprotected Backups:

Messages generally stored in plain Text on SMTP server and also backups can be created. Even if you delete the message they can be residing on the severs/backup-servers for years. So anyone who accesses these servers can also access or read your message.

Repudiation:

As it is known that email messages can easily be forged so anyone sending you some message can later on deny regarding sending of message and it is very difficult to prove it. This has implications corresponding to emails use as contracts in business communications.

Email spoofing:

Sometime email that pretends to be received from an authentic source but in actual it is send from somewhere else.

Email Spamming:

Spam or junk mail refers to sending of email to no. of persons for any advertisement purpose or for some malicious intent. To send spam often lists are created by searching data from Internet, or by stealing mailing list from the internet.

Email bombing:

E-mail "bombing" is refers to sending identical mail repeatedly by abusers to a particular address/user.

Sending threats:

Threatening mails are sending to users which disturb their state of mind or to provoke them to take some wrong step. Sometimes false statements are also forwarded to third parties or users to injure the reputation of some particular person. It is called as Defamation, a communication is not considered defamatory unless it is forwarded to someone other than the target.

Email frauds:

Email Fraud is the intentional deception made for some personal or monetary gain. Emails used as tools to spread malicious software: Emails are also used as tools to spread viruses, worms and other malicious software. They are attached to your emails as attachment, when you click on them they attack your computer or browser.

RESULT:

The main aim is to analyze the security issues and threats in e-mail application in detail is completed successfully.

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

AIM:

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

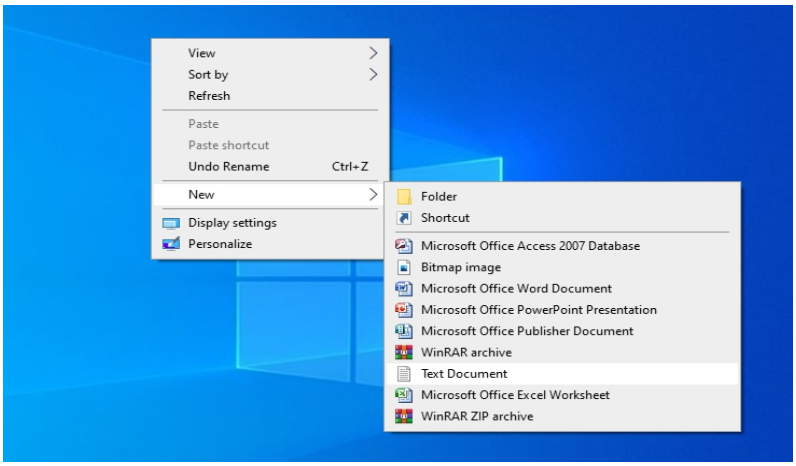
PROCEDURE:

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

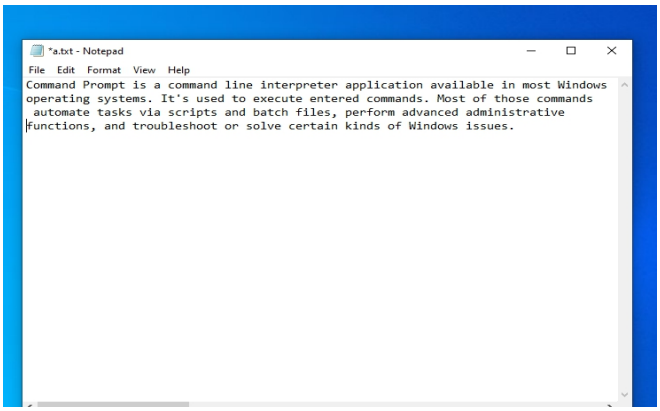
2. Suppose you have to hide a text file “A.txt” with the image file “B.jpg” and combine them in a new file as “C.jpg”. Where “C.jpg” is our output file which contains the text hidden in the image file**.**

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

Example: a.txt is created

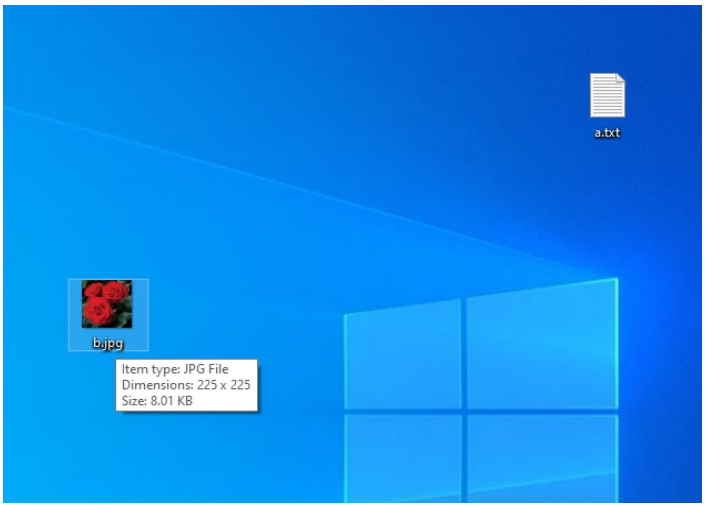


Step2: Type the content which you need to hide in the image and save it

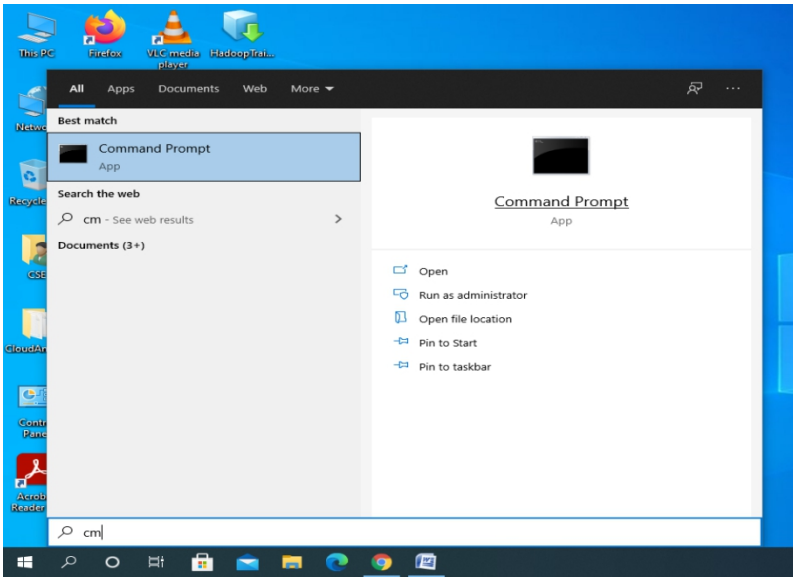


Step 4: Create an image file and save it with the extension .jpg

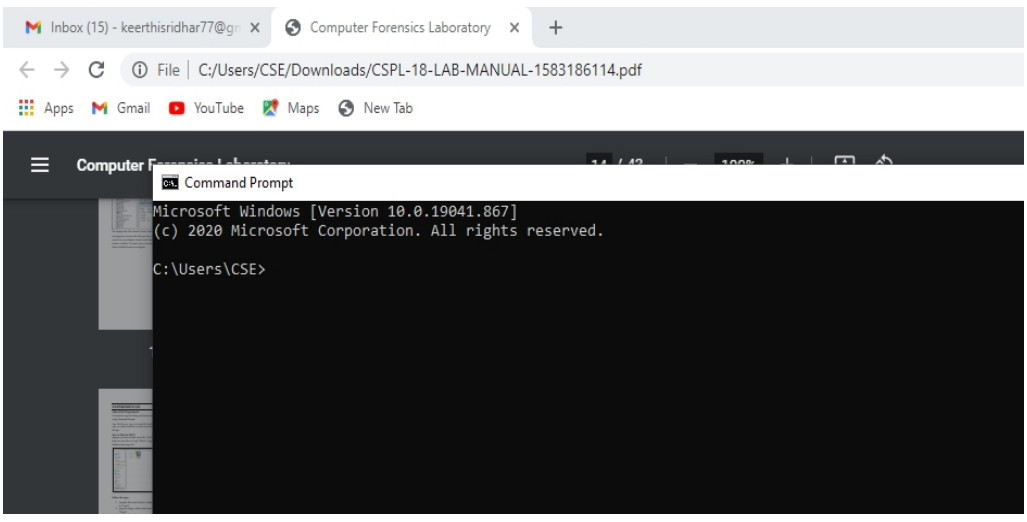
Example: b.jpg is created



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

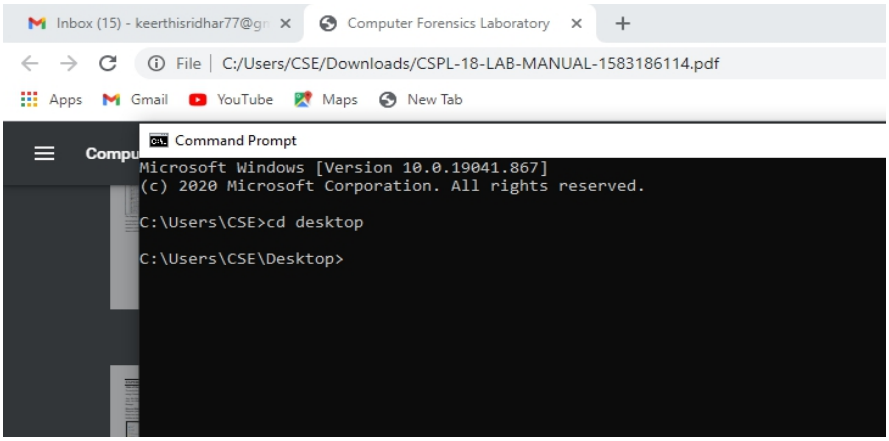


Step 6: Open the command prompt a black working place will be available (or) press ctrl+r and type cmd and hit enter.

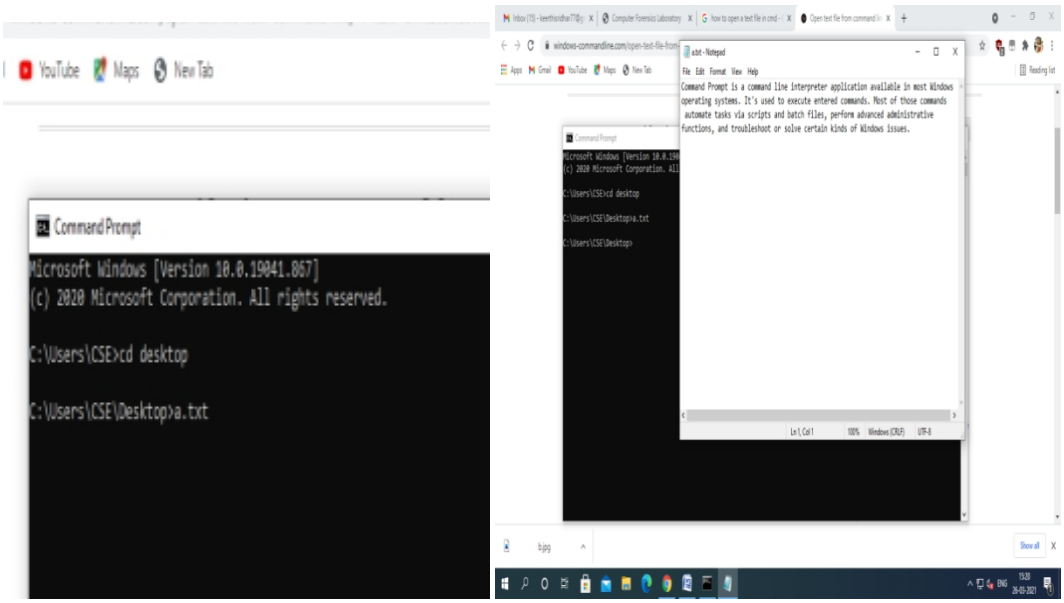


Step 7: Move to the folder where the two are located the CD command is used to enter in to the folder.

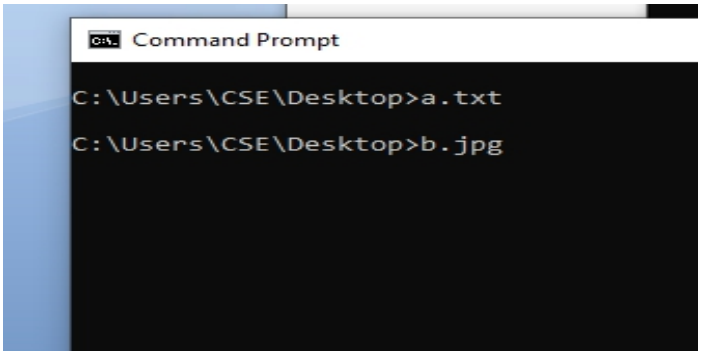
>>cd desktop

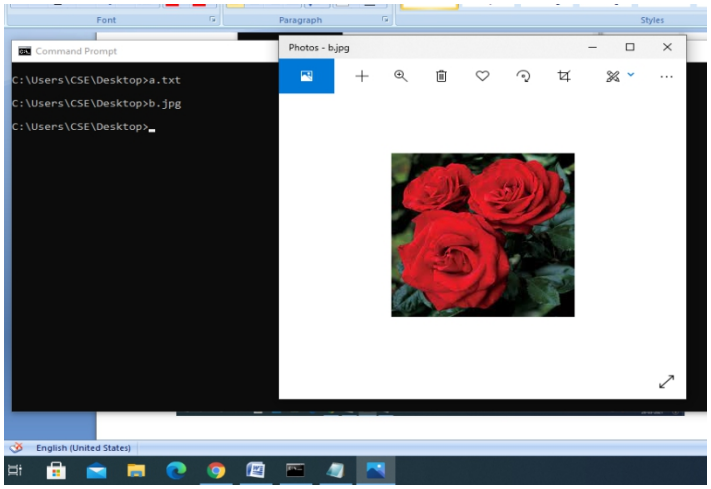


Step 8: Open the text file by its file name Example a.txt then txt file will get open



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

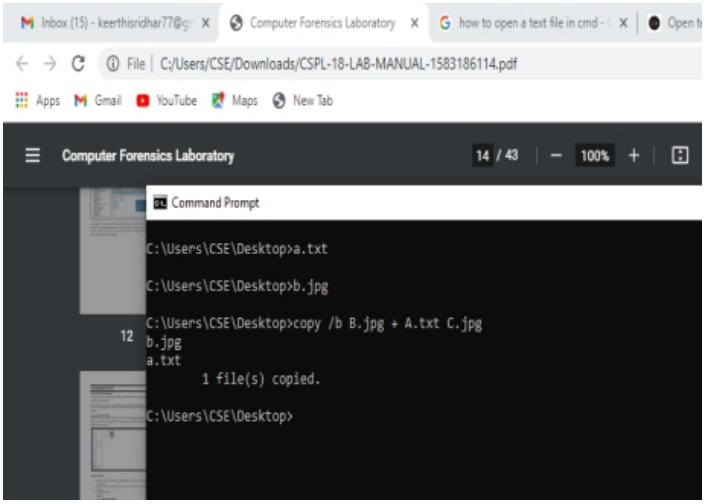




Step 10: Now type the following

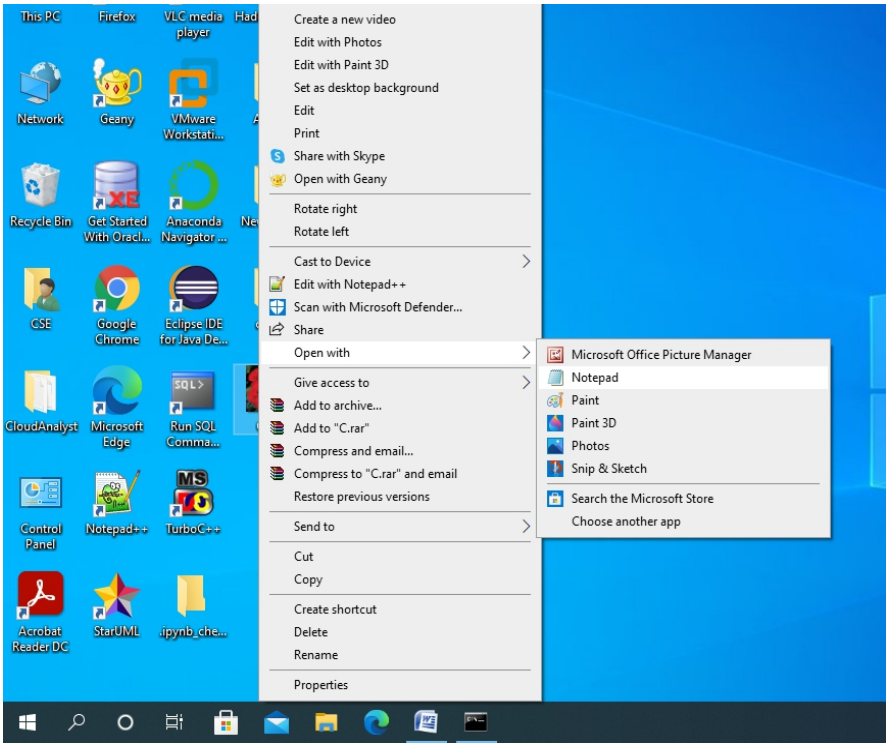
Syntax: copy /b Name-of-file-containing-text-you-want-to-hide.txt + Name-of-initialimage.jpg Resulting-image-name.jpg

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

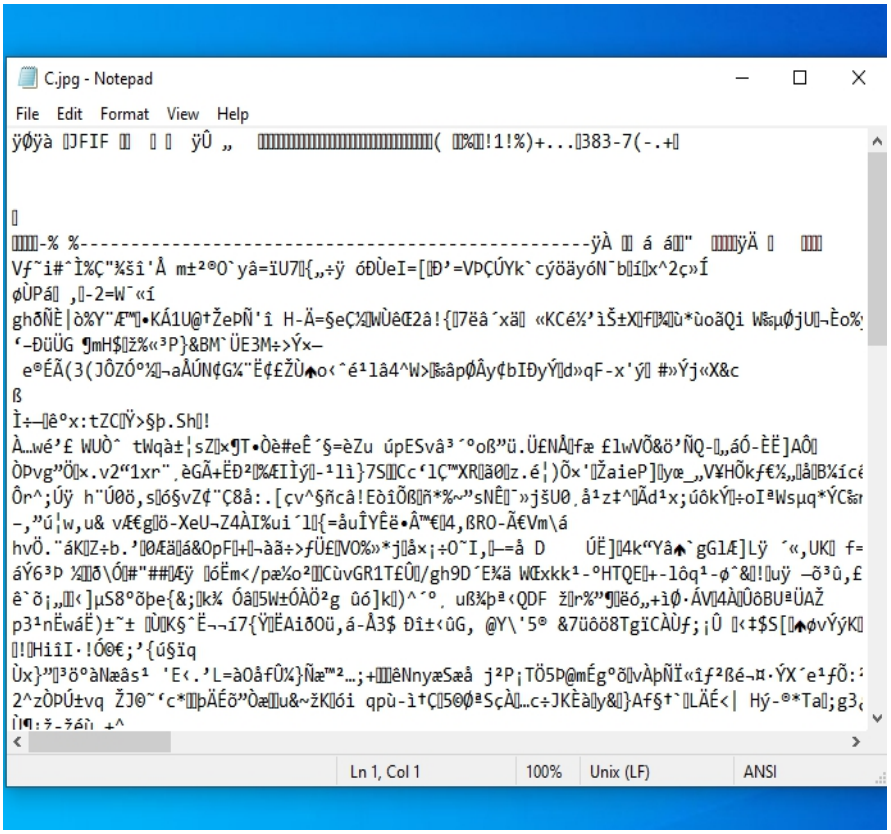


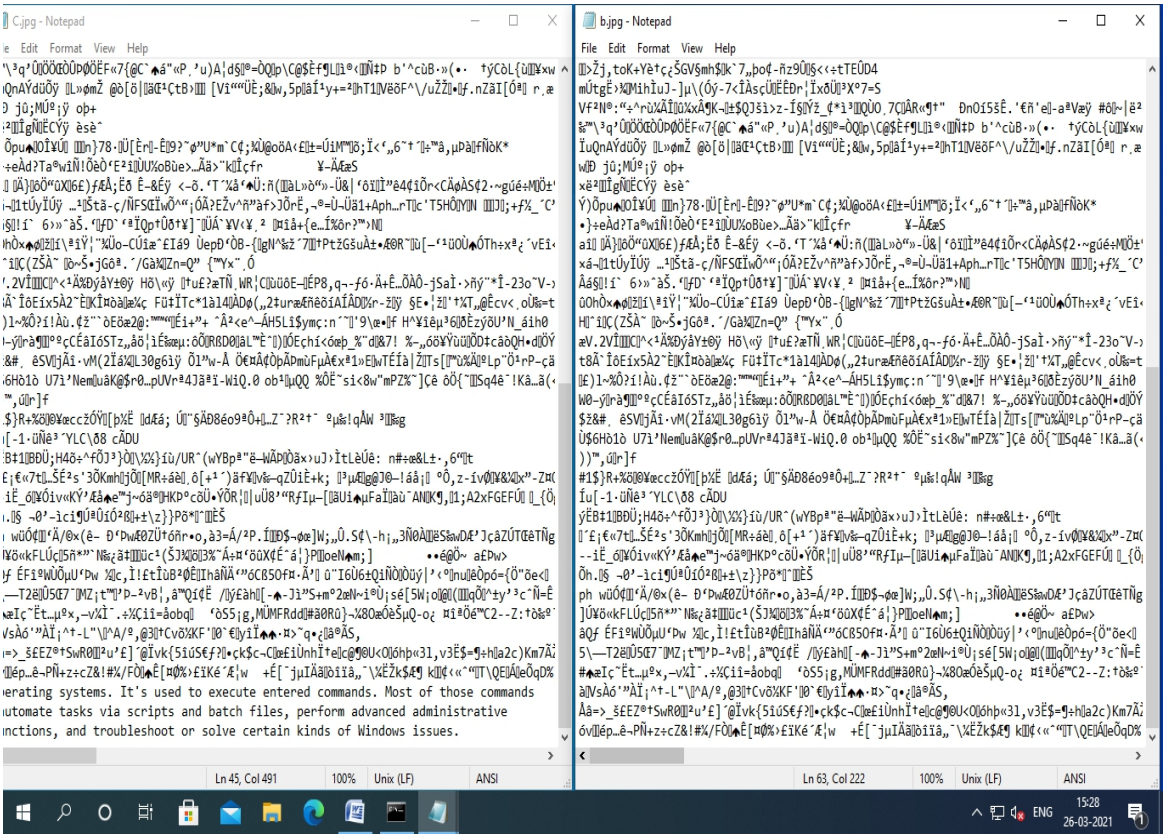
Step 11: locate C.jpg file from where you want to retrieve text data

Step 12: Right-click and open with notepad



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





RESULT:

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