Network Security and Forensics

Lab Session 1

Submitted To:-

Dr. Lokesh Chauhan Sir

Submitted By:-

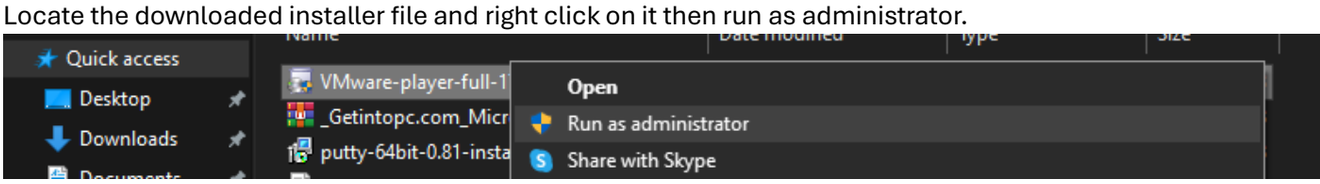
Saloni Rangari

M.Tech. AIDS (CS)

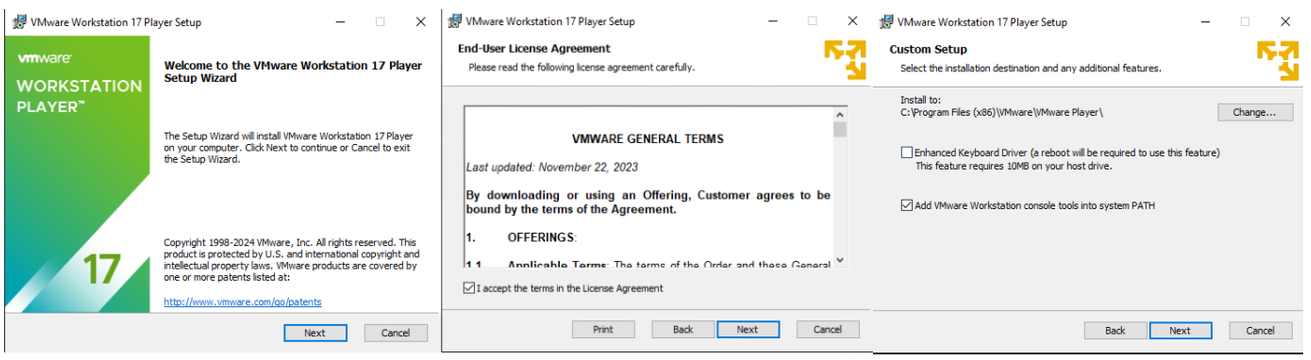
Assignment 1: Install VMware workstation for Linux or windows.

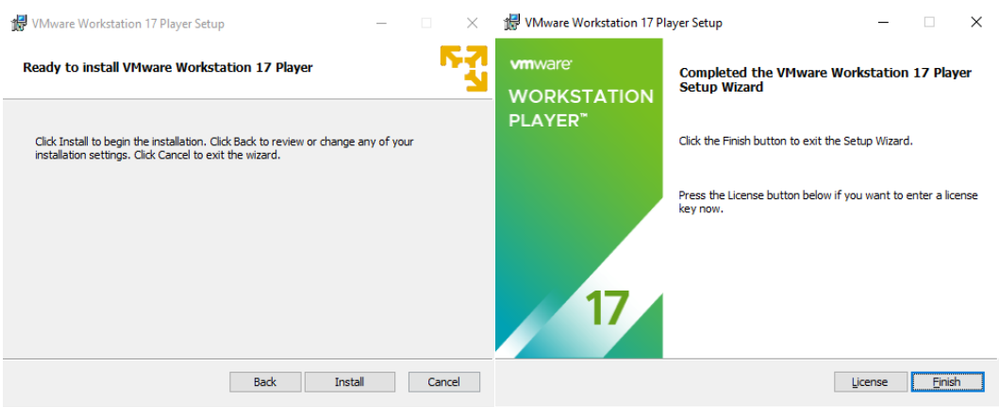
Steps to install VMware Workstation :

1) Go to the official **VMware website**. (https://www.vmware.com/)
2) Log in to the Broadcom support portal. If you do not have an account, you may need to create one.
3) After logging in, navigate to the search bar and type "VMware Workstation"
4) Find the latest version of VMware Workstation Pro suitable for personal use (e.g. v17.52) and click on it.
5) Scroll down to find the download link. Ensure you check any necessary boxes (if applicable) and click the download button to start downloading the installer.
6) Locate the downloaded installer file and right click on it then run as administrator.

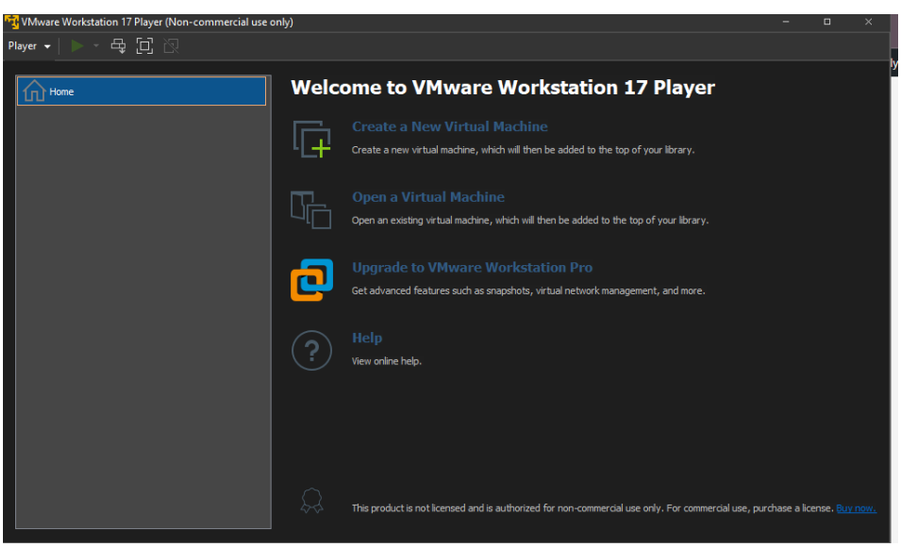


7) Installation Process:
   i) Follow the installation prompts
   ii) Click "Next" on the welcome screen.
   iii) Accept the End User License Agreement.
   iv) Leave the default settings as they are and continue clicking "Next."
   v) Click "Install" to begin the installation.
   vi) Once the installation is complete, click "Finish" to exit the installer.



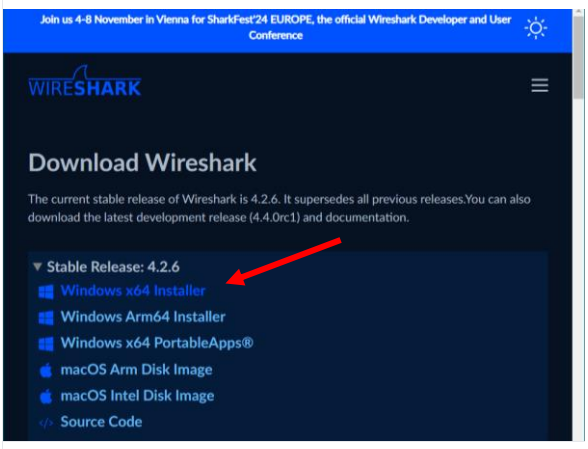


8) Find the VMware Workstation Pro icon on your desktop or in the Start menu and double-click to launch the application.
9) You can now create and manage virtual machines within VMware Workstation Pro.

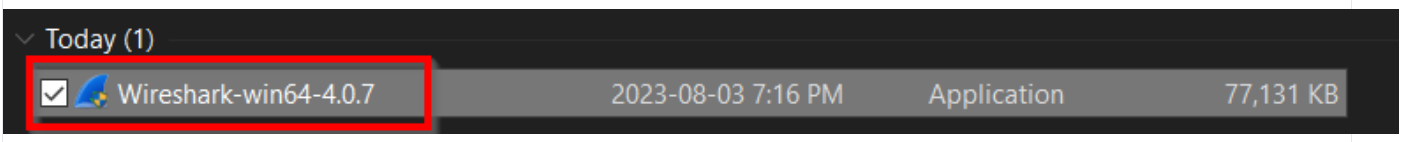


Assignment 2: Install Wireshark for Linux or windows.

1. Visit the official Wireshark download page at wireshark.org.

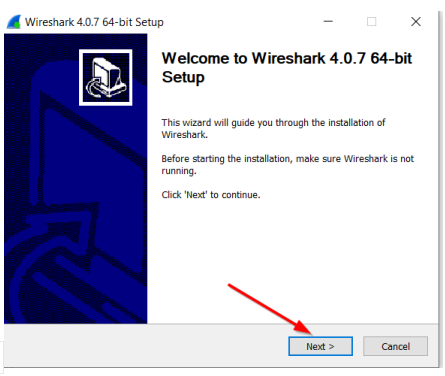


2. Locate the downloaded installer file and click on it to start the installation.

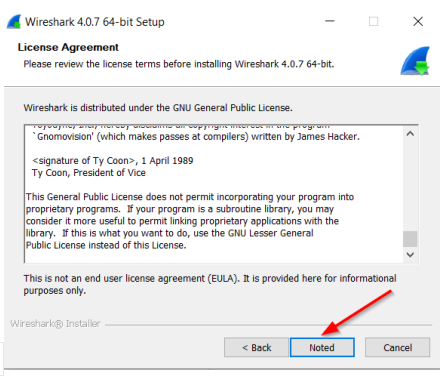


3. Installation Process:

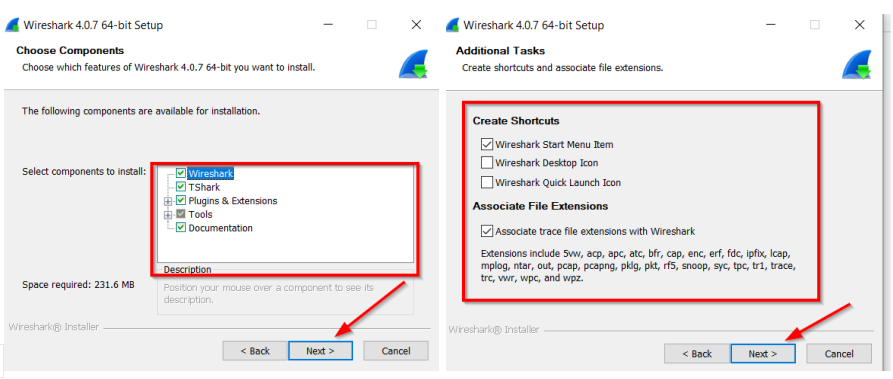
- Click "Next" on the welcome screen.



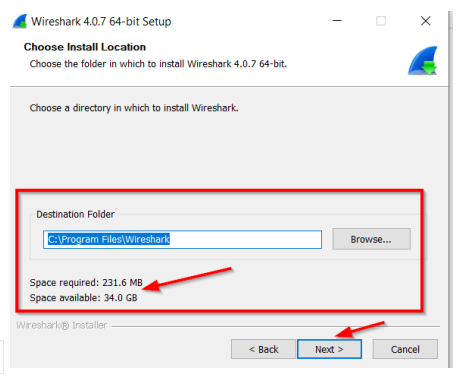
- Accept the End User License Agreement.



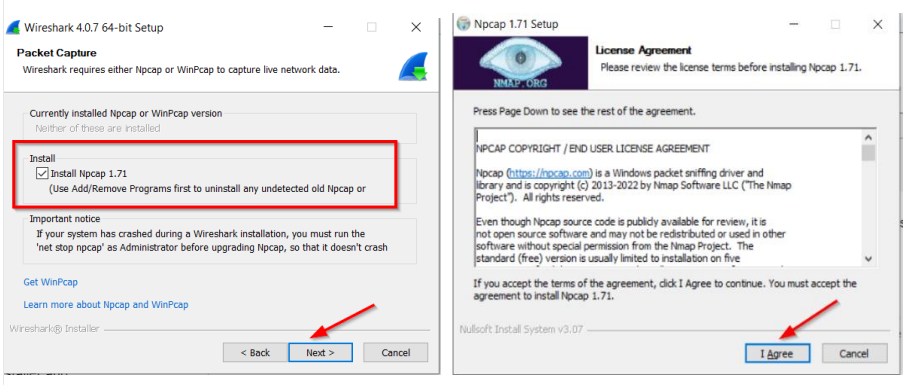
- Choose the components you want to install.



- Select the installation directory and click "Next."

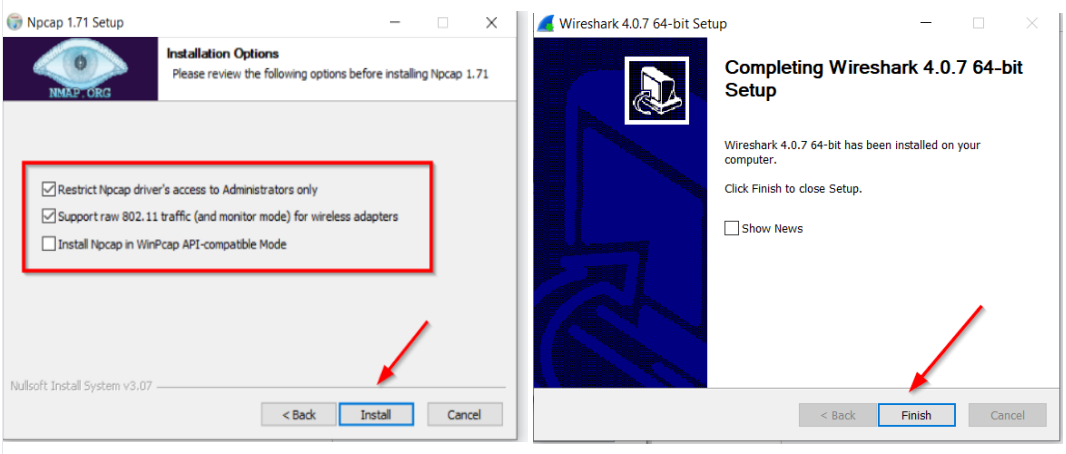


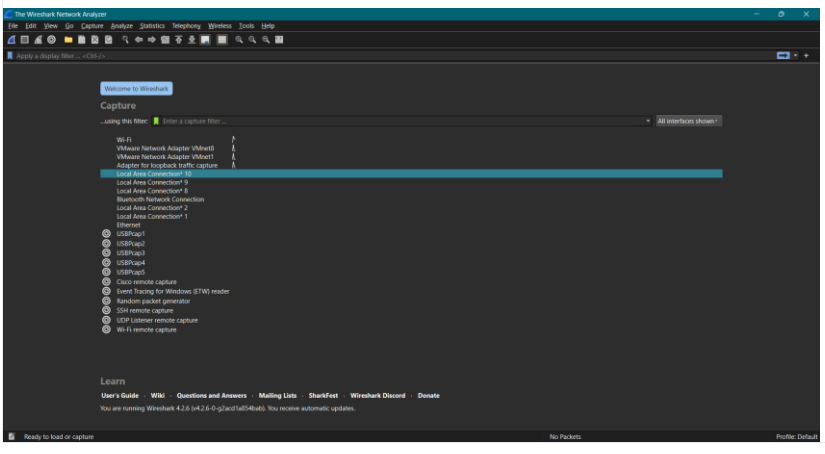
- During installation, you may be prompted to install WinPcap or Npcap (recommended for capturing packets). Follow the instructions to install it.



- Click "Finish" to complete the installation process.

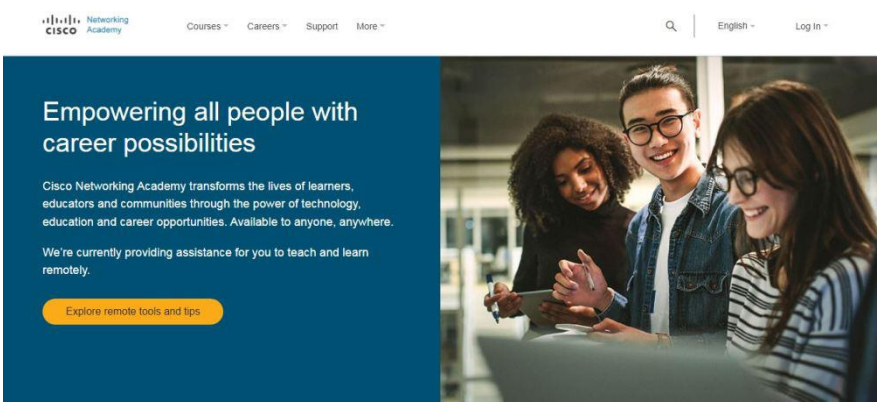
4. Find Wireshark in your Start menu or on your desktop and double-click to launch.



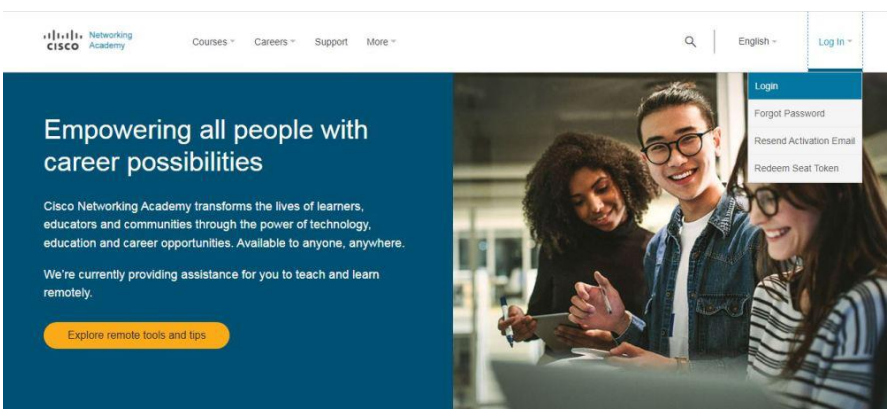


Assignment 3: Install Cisco Packet Tracer.

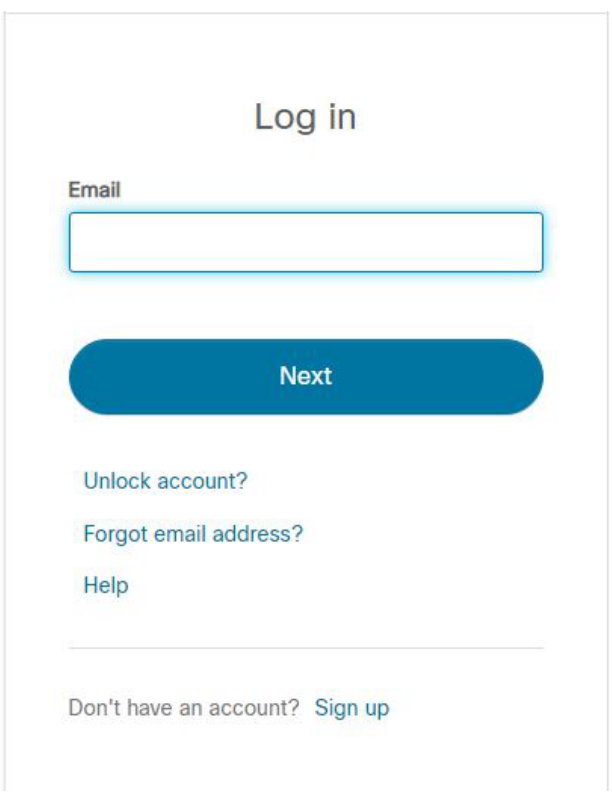
Step 1: Visit the official website of Netacad using any web browser.



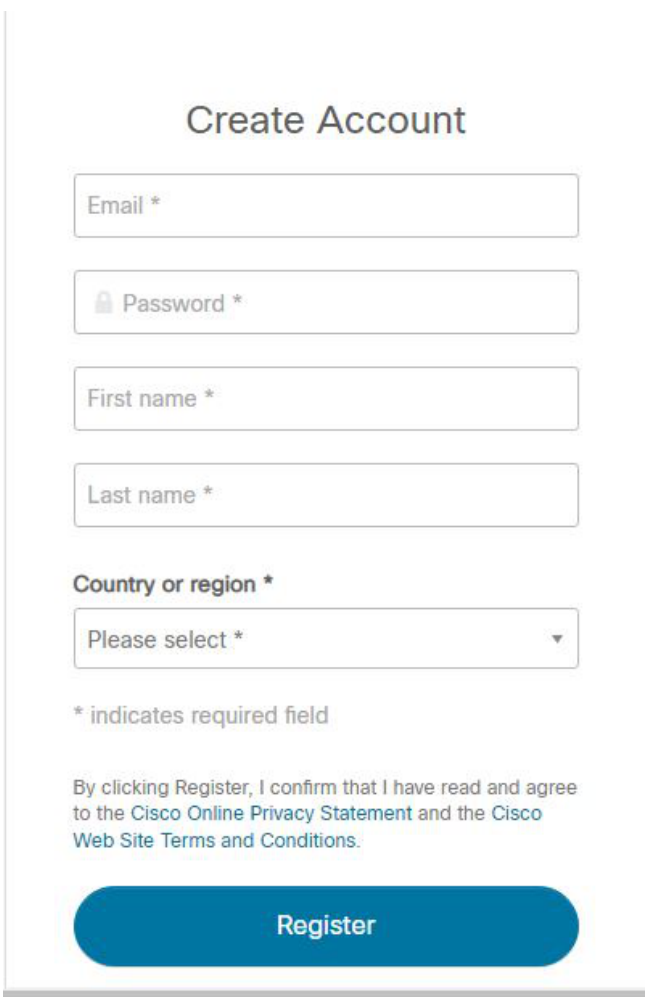
Step 2: Press the login button and select log In option.



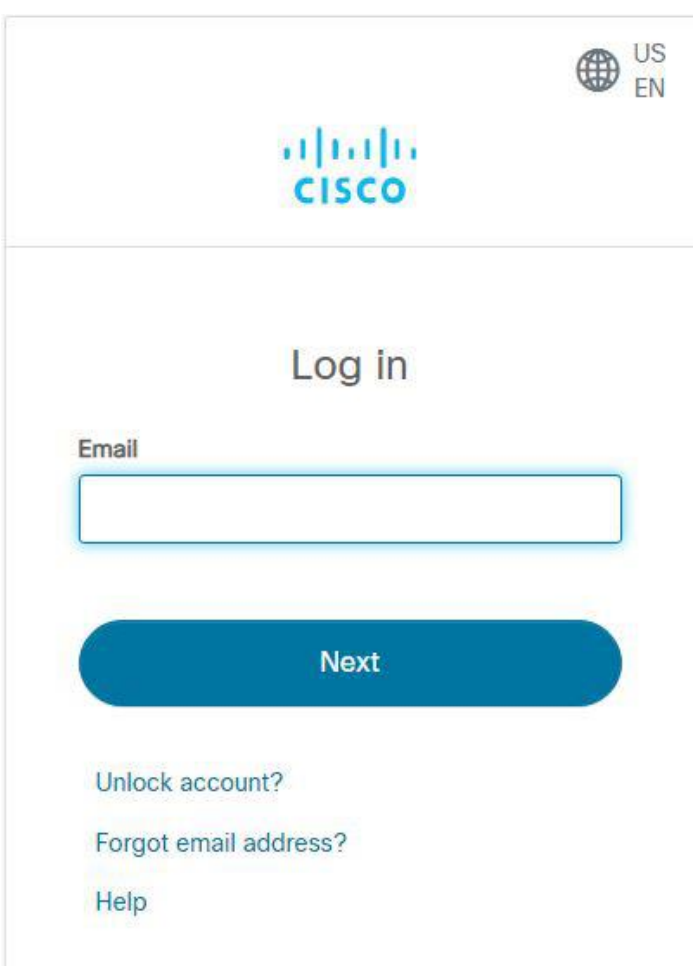
Step 3: Next screen will appear, click on the sign-up option.



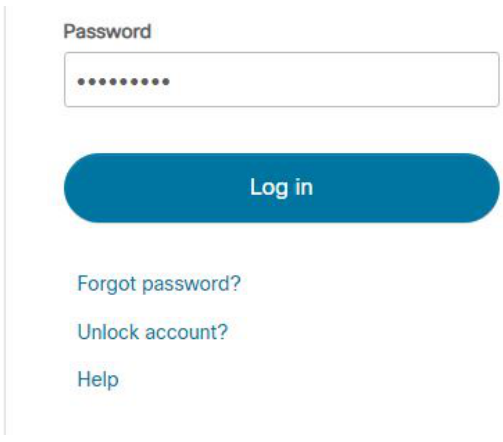
Step 4: Next screen will appear and will ask for email and password and other simple details, fill them and click on Register.



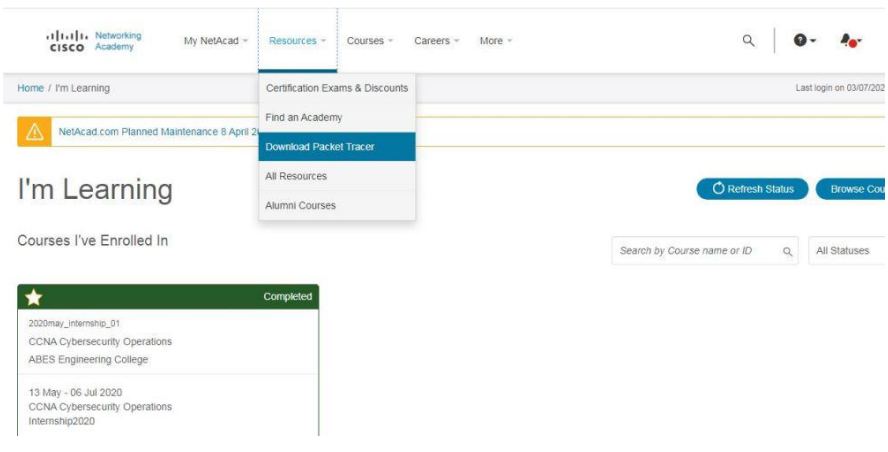
Step 5: Now the login screen appears again so fill in the Email id.



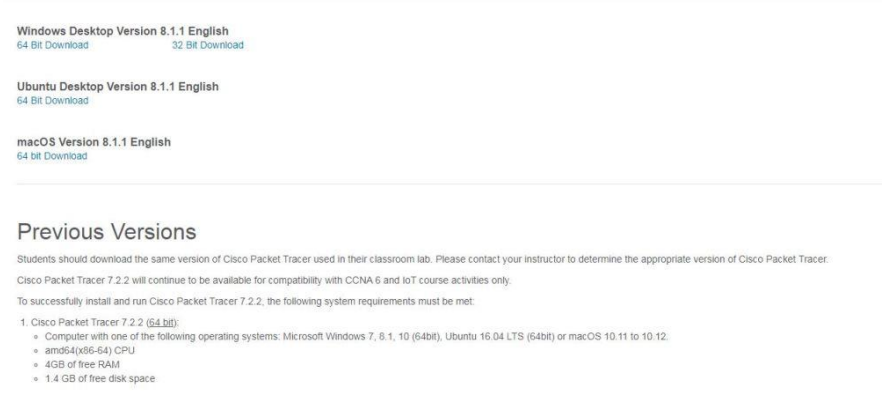
Step 6: On the next screen enter the password and press the Login button.



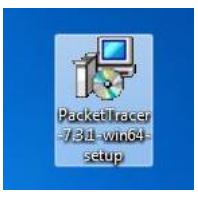
Step 7: Dashboard will initialize, now click on Resources and choose Download Packet Tracer Option.



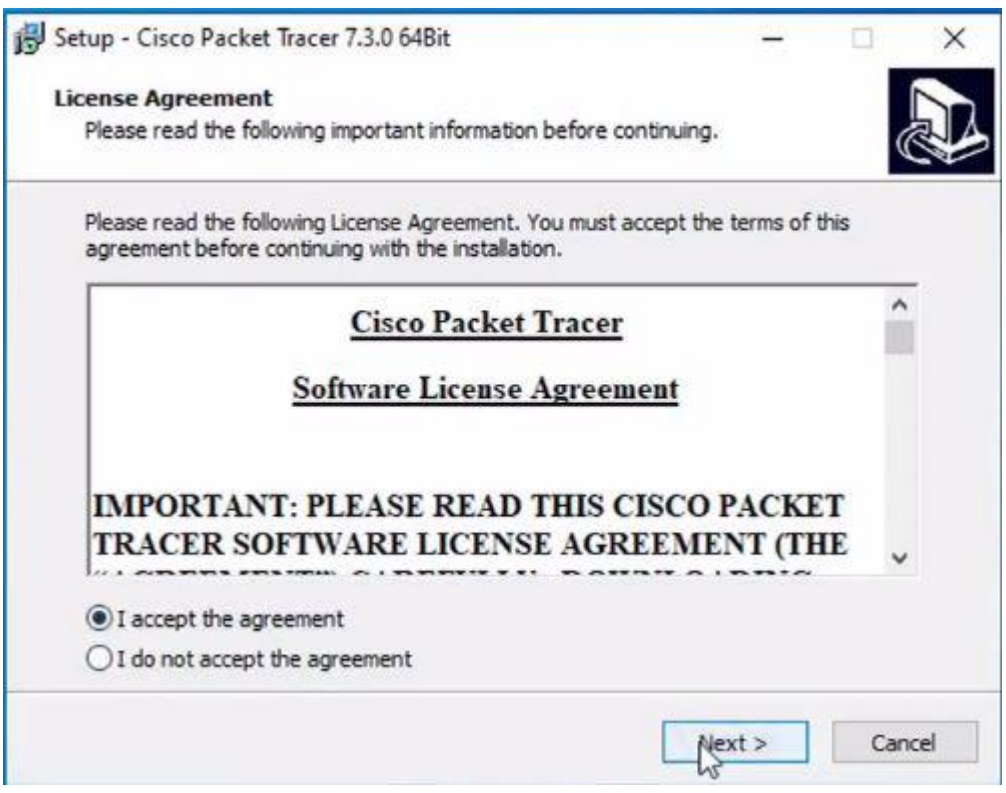
Step 8: On the next web page choose the operating system to download the packet tracer. Downloading will start automatically.



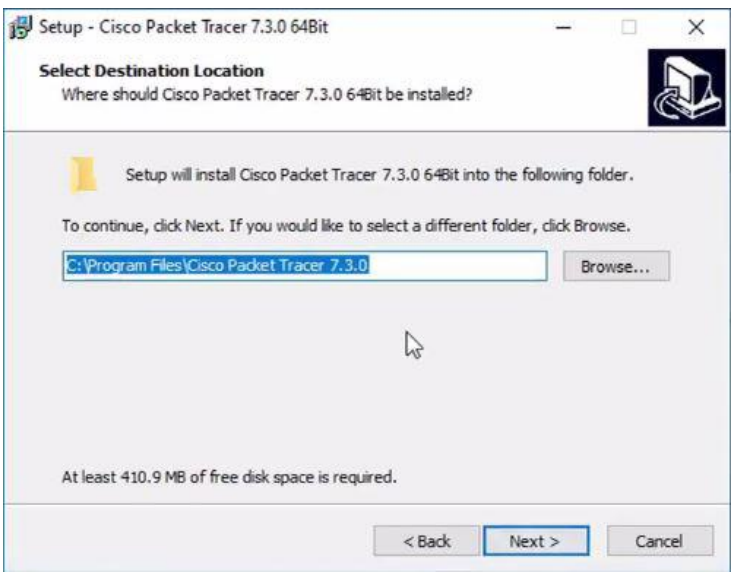
Step 9: Check for the executable file in your system and run it.



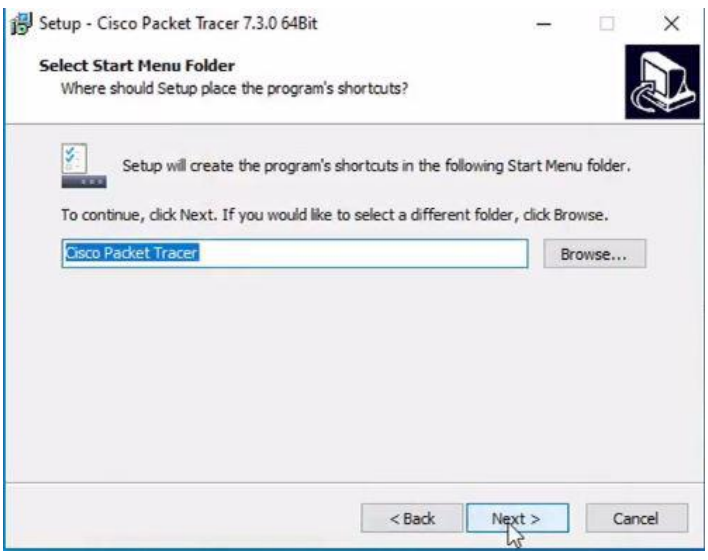
Step 10: Next screen is of License Agreement so Click on I accept the license.



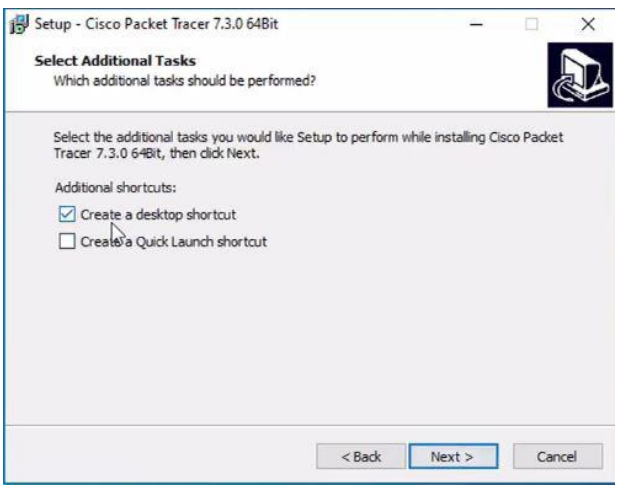
Step 11: Choose the installing location which has sufficient space.



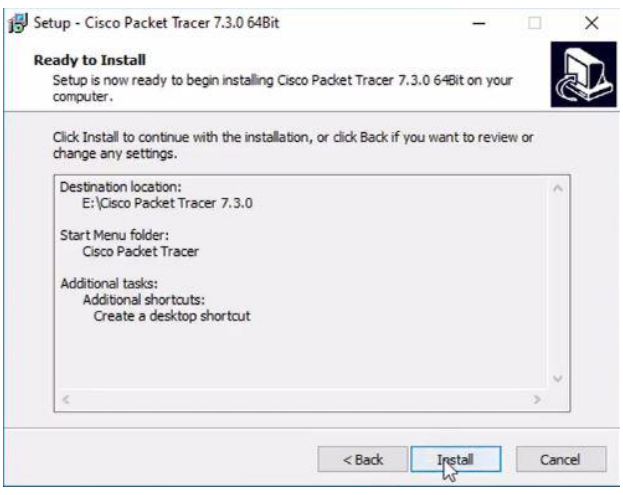
Step 12: Select the start menu folder and click the Next button.



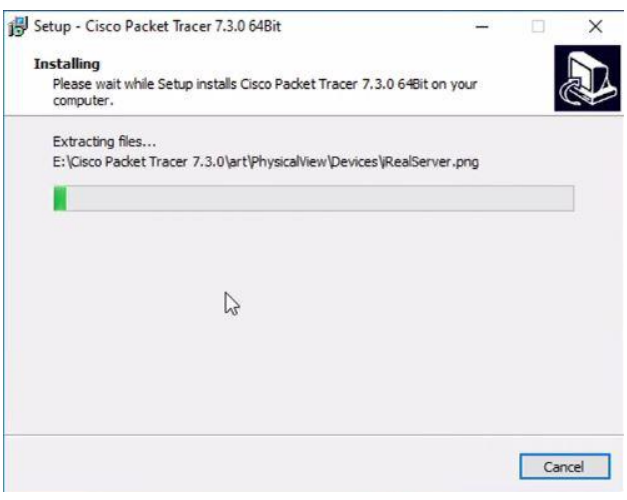
Step 13: Check the box for creating a desktop icon and click on the Next button.



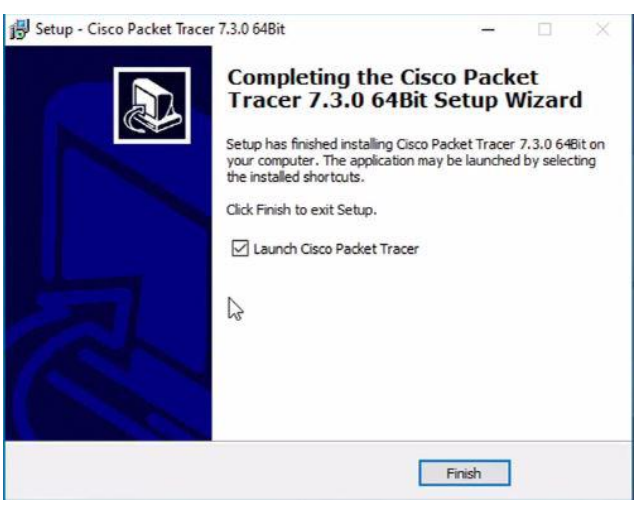
Step 14: Now packet tracer is ready to install so click on the Install button.



Step 15: The installation process will start and will hardly take a minute.

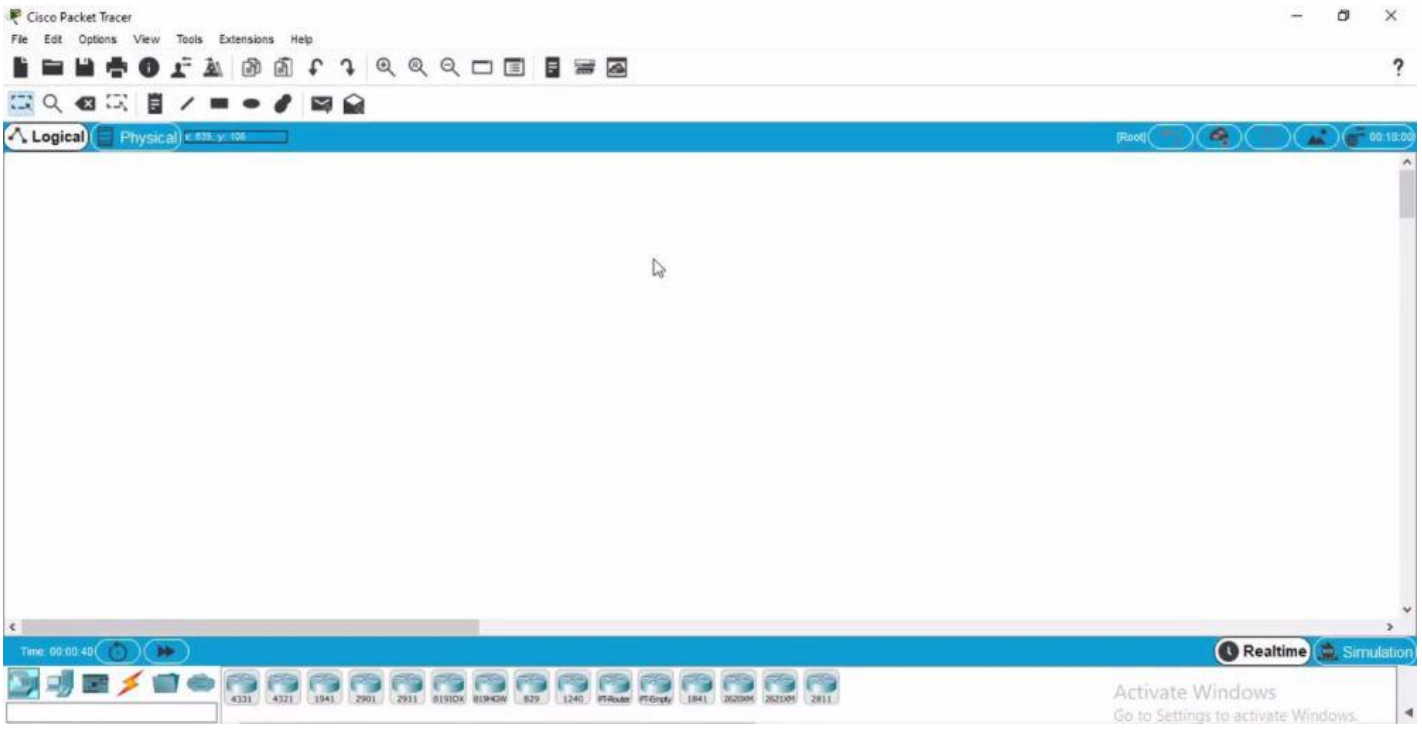


Step 16: Click on the Finish button to complete the installation.



Step 17: An icon is created on the desktop so run it.

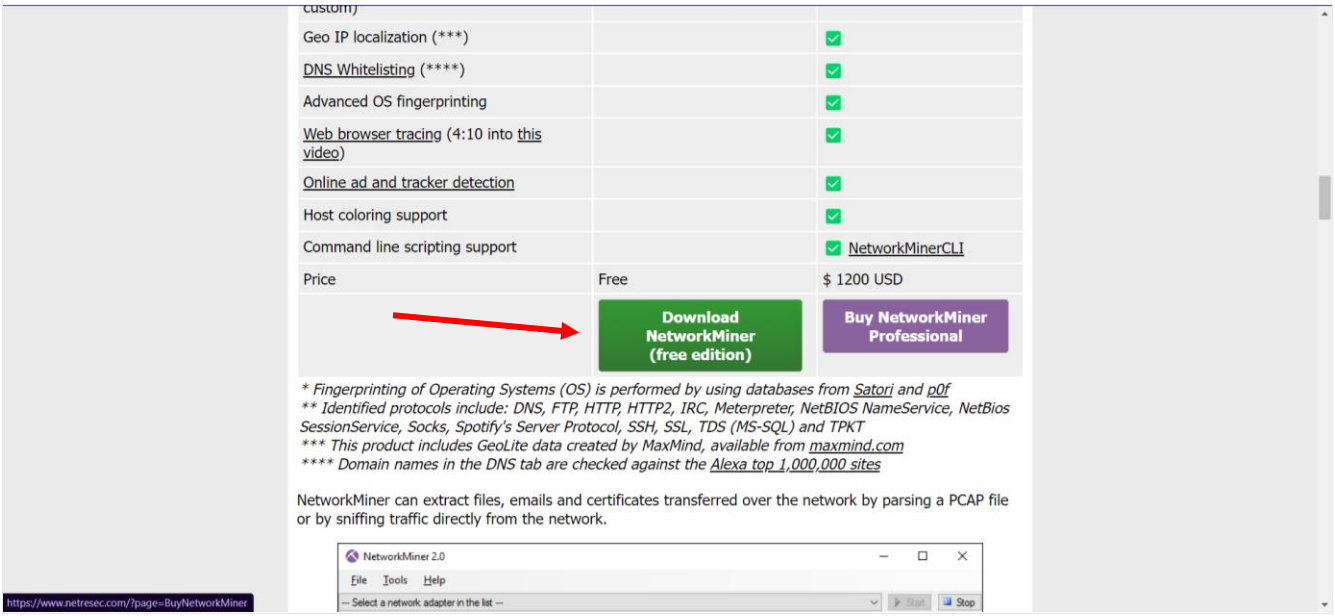
Step 18: Cisco Packet Tracer is ready to use.



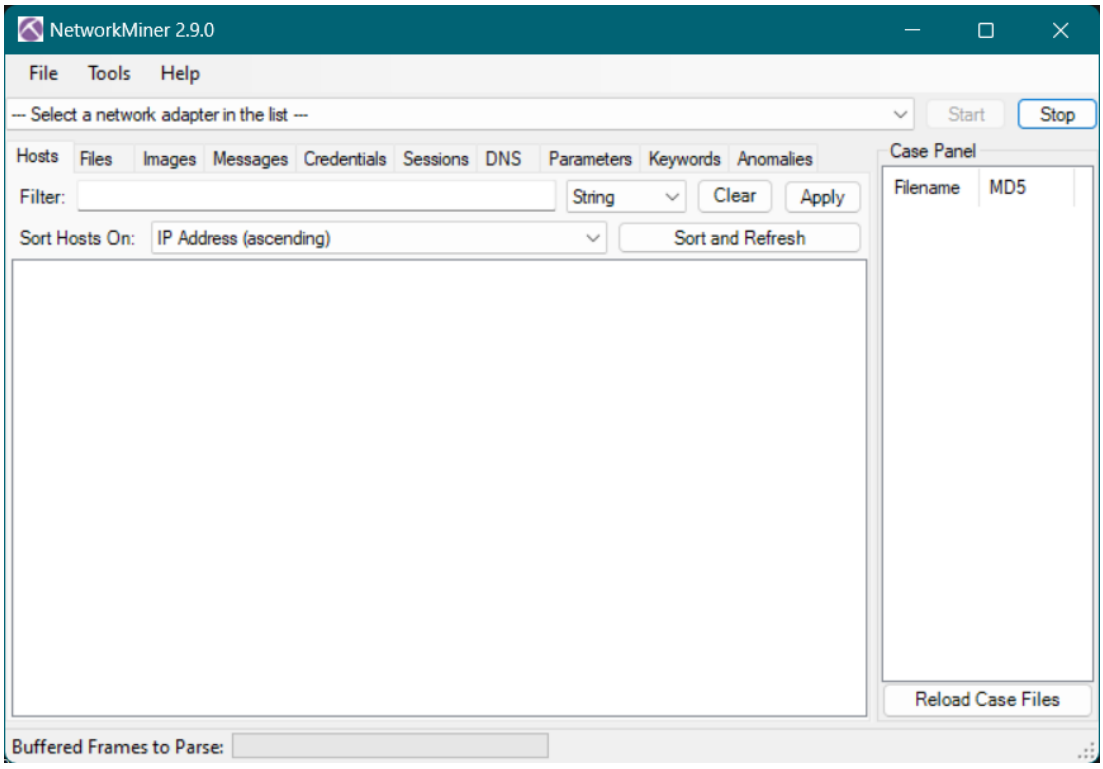
Assignment 4: Install NetworkMiner

To install NetworkMiner on Windows, follow these steps:

1. Visit the official NetworkMiner website at netresec.com and scroll to the bottom of the page to find the download link for the free version. Click the link to download the ZIP file.



2. Once the download is complete, locate the downloaded ZIP file in your downloads folder. Right-click the file and select "Extract All" to unzip it. Choose a destination folder (e.g., C:\Program Files\NetworkMiner) and extract the contents.
3. Navigate to the folder where you extracted NetworkMiner. Locate the NetworkMiner.exe file. Right-click on it and select "Run as administrator" to launch the application with the necessary permissions.
4. In NetworkMiner, select the network interface you want to monitor (e.g., loopback or Ethernet) and start capturing packets. You can do this by clicking on the "Start" button.
5. Once you start capturing, NetworkMiner will display the captured packets. You can analyze the data in real-time or save the capture for later analysis.



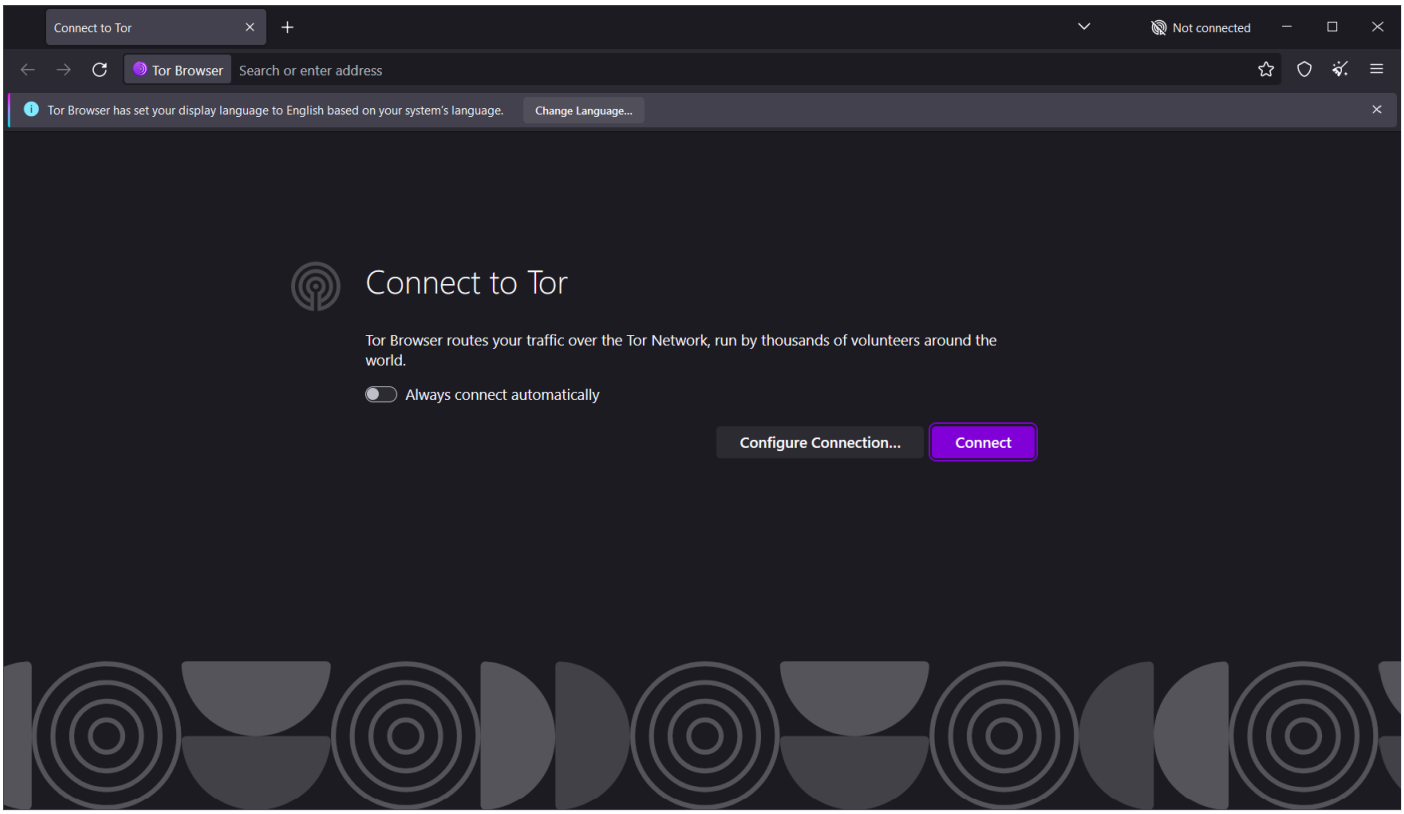
Assignment 5: Install ELK Stack.

Prerequisites:
Ensure you have Java JDK installed. The ELK Stack comes with a bundled JDK, but you can also install it separately if preferred.

1) Step 1: Download the ELK Stack Components
   a. **Download Elasticsearch**:
   b. Visit the official Elasticsearch download page.
   c. Select the Windows version and download the ZIP package.
   d. **Download Logstash**:
   e. Go to the Logstash download page.
   f. Download the Windows ZIP package.
   g. **Download Kibana**:
   h. Visit the Kibana download page.
   i. Download the Windows ZIP package.
2) Step 2: Install Elasticsearch
   a. **Extract the ZIP File**:
   b. Extract the downloaded Elasticsearch ZIP file to your desired location (e.g., C:\ELK\Elasticsearch).
   c. **Start Elasticsearch**:
   d. Open Command Prompt as Administrator.
   e. Navigate to the bin directory of the extracted Elasticsearch folder:
   f. bash
   g. cd C:\ELK\Elasticsearch\bin
   h. Run the following command to start Elasticsearch:
   i. bash
   j. elasticsearch.bat
   k. Confirm that Elasticsearch is running by visiting http://localhost:9200 in your web browser.
3) Step 3: Install Logstash
   a. **Extract the ZIP File**:
   b. Extract the downloaded Logstash ZIP file to your desired location (e.g., C:\ELK\Logstash).
   c. **Create a Configuration File**:
   d. In the Logstash directory, create a configuration file named logstash.conf in the config folder, specifying your input, filter, and output settings.
   e. **Start Logstash**:
   f. Open Command Prompt as Administrator.
   g. Navigate to the bin directory of the Logstash folder:
   h. bash
   i. cd C:\ELK\Logstash\bin
   j. Run Logstash with the configuration file:
   k. bash
   l. logstash.bat -f ..\config\logstash.conf
4) Step 4: Install Kibana
   a. **Extract the ZIP File**:
   b. Extract the downloaded Kibana ZIP file to your desired location (e.g., C:\ELK\Kibana).
   c. **Start Kibana**:
   d. Open Command Prompt as Administrator.
   e. Navigate to the bin directory of the Kibana folder:
   f. bash
   g. cd C:\ELK\Kibana\bin
   h. Run the following command to start Kibana:
   i. bash
   j. kibana.bat
   k. Access Kibana by visiting http://localhost:5601 in your web browser.
5) Step 5: Verify the Installation
   a. Ensure that all components are running properly by checking their respective URLs:
   b. Elasticsearch: http://localhost:9200
   c. Kibana: http://localhost:5601

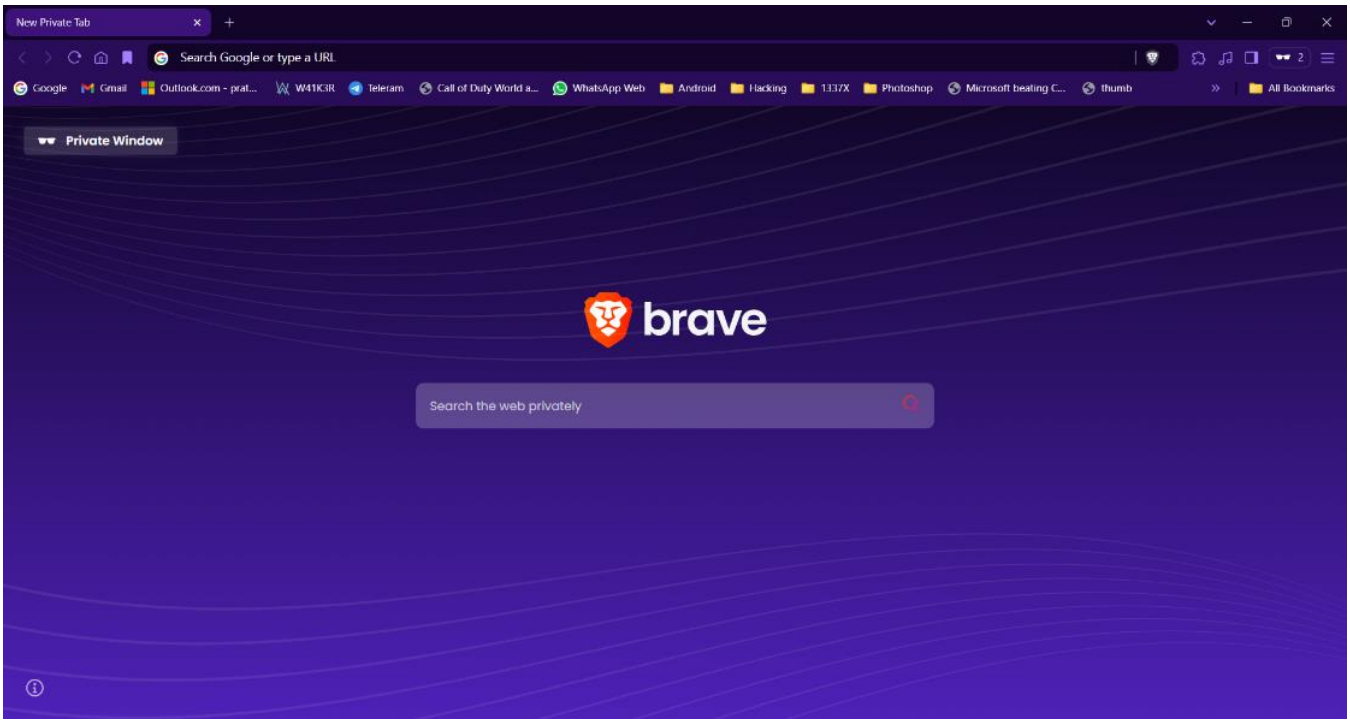
Assignment 6: Install and perform various settings in following browsers:

- **TOR Browser**
  1) To install the Tor Browser on Windows, follow these steps:
  2) Visit the official Tor Project website at torproject.org.
  3) Click on the "Download" button for Windows to download the installer.
  4) Once the download is complete, locate the downloaded file (usually named TorBrowser-install-win64-x.x.x_en-US.exe) in your downloads folder.
  5) Double-click the installer file to run it.
  6) A setup window will appear. Select your preferred language and click "OK."
  7) Choose the installation directory where you want to install the Tor Browser. The default location is usually fine. Click "Install" to proceed.
  8) Wait for the installation process to complete. This may take a few moments.
  9) Once the installation is finished, the Tor Browser will open automatically. If it doesn't, you can find it in your Start menu or on your desktop.
  10) When the Tor Browser opens, click the "Connect" button to connect to the Tor network. This may take a minute or two.
  11) After connecting, you can start using the Tor Browser to browse the internet anonymously.

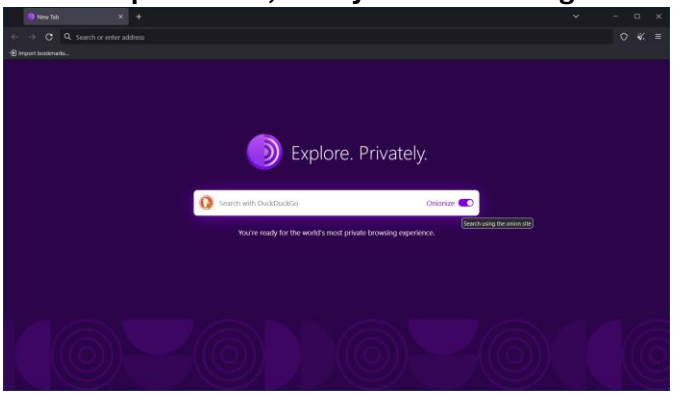


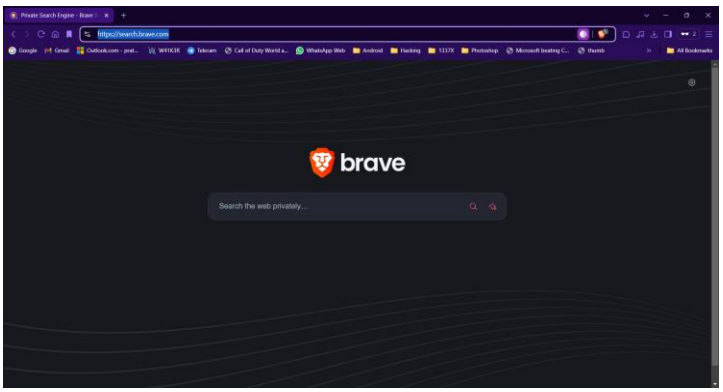
- **Brave Browser**
  Steps to install the Brave Browser on Windows:

  1) Visit the official Brave website at brave.com and click on the download button for Windows. This will download the Brave installer file.
  2) Locate the downloaded installer file (usually named BraveBrowserSetup.exe) in your downloads folder. Double-click the file to run it.
  3) If prompted by User Account Control (UAC), click "Yes" to allow the installer to make changes to your device.
  4) The installation process will begin. Wait for it to complete.
  5) Once the installation is finished, you will see a Brave window open automatically. You can also find the Brave icon on your desktop or in the Start menu.
  6) Follow the on-screen prompts to set up your Brave browser preferences, including syncing with your account if desired.



- **explore safe, anonymous browsing.**





Assignment 7: Open the website, www.cert-in.org.in

(i) write the procedure to report an incident.

1. **Reporting of a Security Incident**

   A computer security incident is any adverse event whereby some aspect of a computer system is threatened viz. loss of confidentiality, disruption of data or system integrity, denial of service availability. Any organisation or corporate using computer systems and networks may be confronted with security breaches or computer security incidents. By reporting such computer security incidents to CERT-In the System Administrators and users will receive technical assistance in resolving these incidents. This will also help the CERT-In to correlate the incidents thus reported and analyse them; draw inferences; disseminate up-to-date information and develop effective security guidelines to prevent occurrence of the incidents in future.

2. **Reporting of an incident**

   System Administrators can report an adverse activity or unwanted behaviour which they may feel as an incident to CERT-In. They may use the following channels to report the incident.

   - E-mail: incident@cert-in.org.in

   - Helpdesk: +91-1800-11-4949

   - Fax: +91-1800-11-6969

3. **Contents of Incident Report**

   The following information (as much as possible) may be given while reporting the incident.

   - Time of occurrence of the incident

   - Information regarding affected system/network

   - Symptoms observed

   - Relevant technical information such as security systems deployed, actions taken to mitigate the damage etc.

4. **Verification**

   CERT-In will verify the authenticity of the report.

   We have to fill the form

Incident Reporting Form

I am: ☐ the effected entity ☐ reporting incident affecting other entity			
Contact Information of the Reporter			
Name & Role/Title	☐ Individual ☐ Organization		
Organization name (if any)			
Contact No.		Email:	
Address:			
Basic Incident Details			
Affected entity (if not same as reporting entity above)			
Incident Type			
☐ Targeted scanning/probing of critical networks/systems ☐ Compromise of critical systems/information ☐ Unauthorised access of IT systems/data ☐ Defacement or intrusion into the website ☐ Malicious code attacks ☐ Attack on servers such as Database, Mail and DNS and network devices such as Routers ☐ Identity Theft, spoofing and phishing attacks ☐ DoS/DDoS attacks ☐ Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks ☐ Attacks on Application such as E-Governance, E-Commerce etc.	☐ Data Breach ☐ Data Leak ☐ Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers ☐ Attacks or incident affecting Digital Payment systems ☐ Attacks through Malicious mobile Apps ☐ Fake mobile Apps ☐ Unauthorised access to social media accounts ☐ Attacks or malicious/ suspicious activities affecting Cloud computing systems/servers/software/applications	☐ Attacks or malicious/suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Block chain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones ☐ Attacks or malicious/ suspicious activities affecting systems/ servers/software/ applications related to Artificial Intelligence and Machine Learning ☐ Other (Please Specify) --- ---
Is the affected system/network critical to the organization's mission? (Yes / No). (Brief details.)			
Basic Information of Affected System (Provide information that is readily available.)	Domain/URL: IP Address: Operating System: Make/ Model/Cloud details: Affected Application details (If any): Location of affected system (including City, Region & Country): Network and name of ISP:		
Brief description of Incident:	Occurrence date & time (dd/mm/yyyy hh:mm): Detection date & time (dd/mm/yyyy hh:mm):		

(ii) write the procedure to report about the vulnerabilities.

1.Introduction

Responsible Vulnerability Disclosure and Coordination refers to the process of collection, analysis, mitigation coordination with researchers/finders and vendors leading to the public disclosure of newly identified cybersecurity vulnerabilities. The purpose of Responsible Vulnerability Disclosure and Coordination is to ensure that affected vendors/OEMs get sufficient time to remediate the vulnerability. Indian Computer Emergency Response Team (CERT-In) collaborates with researchers, cybersecurity organizations, academic institutions, vendors/OEMs, and CERT's all over the world on handling of reported vulnerabilities. In this direction, CERT-In has formulated this Responsible Vulnerability Disclosure and Coordination Policy with an aim to strengthen trust in "Digital India", "Make in India" as well as to encourage responsible vulnerability research in the Country.

2. Reporting vulnerabilities to CERT-In

i) Security vulnerabilities in any product can be sent to us via email at vdisclose@cert-in.org.in. CERT-In accepts PGP Encrypted emails and attachments.
ii) The details of the public key are hereunder:
   a) - Email ID: vdisclose@cert-in.org.in
   b) - Key ID: 0x3B4E082C
   c) - Key Type: RSA
   d) - Expires Date: 2024-12-31
   e) - Key Size: 4096/4096
   f) - Fingerprint: 6927 2217 D8D4 0208 6B1C 23E9 CE29 6AE7 3B4E 082C
   g) - Helpdesk: +91-1800-11-4949 (Toll Free)
   h) - Fax: +91-1800-11-6969
iii) Acknowledgement will be sent within 72 working hours upon receipt of the vulnerability information by CERT-In.

3. Details expected in vulnerability reports

In order to examine and validate the vulnerability, CERT-In will look forward to certain details as indicated below:

i) The product(s) affected
ii) The exact software version or model affected.
iii) Vendor details
iv) Description of the vulnerability along with concise steps to reproduce the reported vulnerability along with supporting evidences such as:
   a) Proof of concept (PoC) and/or
   b) Code sample and/or
   c) Crash reports and/or
   d) Screenshots and Video recording etc.
   e) The impact of exploiting the vulnerability
v) In addition to the above, preferably the following details also may be provided:
   - Other products or software versions likely to be affected
   - How the vulnerability was discovered
   - The tools used for discovering the vulnerability
   - Information on any known exploit
   - Time constraints with respect to going public about the issue (e.g. article, blog or conference etc.)
   - Whether the vulnerability has already been reported to the vendor / other agency or any plan to do so
   - Whether reporting party wants to remain anonymous during the coordination process
   - Whether reporting party wants mention in the vulnerability note / advisory

6) Following need to be ensured before reporting the issue:
   - The vulnerability must be reproducible on the latest available version or 'supported' version of the product
   - The vulnerability must not be previously known
7) Fill the vulnerability reporting form

certin
Enhancing Cyber Security in India

Vulnerability Reporting Form

Reporter Information	
Name	
Organization name (if any)	
Contact No. (Mobile/Phone)	
Email-id	
Anonimity	☐ YES ☐ NO
Vulnerability Details	
Vulnerable Product Type	☐ Website/Web Application ☐ Mobile App ☐ Software (OS, Server or Client Software) ☐ Hardware / Firmware ☐ SCADA/ PLC ☐ Social Media ☐ Other
Vendor/OEM/Affected Entity	
Product Name & Version	
Type of Vulnerability (e.g. CWE, OWASP Top 10 etc.)	
Vulnerability Description	
How can the vulnerability be exploited? (Steps to reproduce along with appropriate Proof of Concept (PoC)/Code sample/Screenshots /Video recording etc.)	
Vulnerability Impact	
Additional Information	
Issue reported to affected entity?	YES / NO

(iii) Procedure to secure your PC.

1. **Keep up with system and software security updates**

   Regularly install updates to patch vulnerabilities and enhance security features.

2. **Have your wits about you**

   Stay vigilant against phishing attempts and suspicious links or downloads.

3. **Enable a firewall**

   Activate your operating system's firewall to monitor and control incoming and outgoing network traffic.

4. **Adjust your browser settings**

   Configure your browser to block pop-ups, disable third-party cookies, and enhance privacy settings.

5. **Install antivirus and anti spyware software**

   Use reputable security software to detect and remove malware and spyware threats.

6. **Password protect your software and lock your device**

   Use strong, unique passwords for applications and set your device to lock automatically when not in use.

7. **Encrypt your data**

   Use encryption tools to protect sensitive files and data from unauthorized access.

8. **Use a VPN**

   Utilize a Virtual Private Network (VPN) to secure your internet connection and protect your online privacy.

(iv) List down various security related tools and websites with proper explanation. Also install these tools on your system.

A list of various security-related tools and websites with explanations and how to install these tools.

I. Tools

1. Wireshark

Wireshark is a network protocol analyzer that allows you to capture and analyze network traffic in real-time. It is useful for troubleshooting network issues, analyzing security, and more.

Installation:

1. Visit the official Wireshark website at wireshark.org.
2. Download the installer for your operating system (Windows, macOS, or Linux).
3. Run the installer and follow the prompts to complete the installation.

2. Nmap

Nmap (Network Mapper) is an open source tool used to discover hosts and services on a network by sending packets and analyzing the responses. It is commonly used for network discovery, security auditing, and more.

Installation:

1. Visit the official Nmap website at nmap.org.
2. Download the installer for your operating system.
3. Run the installer and follow the prompts to complete the installation.

3. Metasploit

Metasploit is a penetration testing framework that allows you to find and exploit vulnerabilities in a controlled environment. It provides a wide range of tools and exploits for security professionals.

Installation:

1. Visit the official Metasploit website at metasploit.com.
2. Choose the appropriate edition (Community or Pro) and download the installer for your operating system.
3. Run the installer and follow the prompts to complete the installation.

4. Snort

Snort is an open source network intrusion detection and prevention system (NIDS/NIPS). It monitors network traffic for suspicious activity and generates alerts when potential threats are detected. \

Installation:

1. Visit the official Snort website at snort.org.
2. Choose the appropriate version and download the installer for your operating system.
3. Run the installer and follow the prompts to complete the installation.

5. Burp Suite

Burp Suite is a web application security testing platform. It includes tools for intercepting and modifying web traffic, discovering vulnerabilities, and automating security tasks.

Installation:

1. Visit the official Burp Suite website at portswigger.net.
2. Download the installer for your operating system.
3. Run the installer and follow the prompts to complete the installation.

II. Websites

1. CERT-In

The Indian Computer Emergency Response Team (CERT-In) is the national nodal agency for responding to computer security incidents. It provides guidelines, advisories, and resources related to cybersecurity.

Website: cert-in.org.in

2. OWASP

The Open Web Application Security Project (OWASP) is an international non-profit dedicated to web application security. It provides resources, tools, and best practices for secure web development.

Website: owasp.org

3. SANS Institute

SANS Institute is a cooperative research and education organization that specializes in information security and cybersecurity training. It offers courses, certifications, and resources for security professionals.

Website: sans.org

4. US-CERT

The United States Computer Emergency Readiness Team (US-CERT) is a government organization that monitors, analyzes, and responds to cybersecurity threats. It provides alerts, bulletins, and resources related to cybersecurity.

Website: us-cert.gov

5. MITRE ATT&CK

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. It is used for planning security improvements and evaluating security products.

Website: attack.mitre.org

By utilizing these tools and resources, you can enhance your cybersecurity knowledge and skills, as well as improve the security posture of your systems and networks.

Assignment 8: Open the website, http://pgportal.gov.in and write the procedure to file the public grievance.

Step 1: Visit the Website

Open your web browser and go to the URL http://pgportal.gov.in. This will take you to the homepage of the Public Grievances Portal.

Step 2: Click on "Register Grievance"

On the homepage, locate and click on the "Register Grievance" button or link. This will take you to the grievance registration page.

Step 3: Select the Appropriate Ministry/Department

On the grievance registration page, you will be asked to select the ministry or department related to your grievance from a dropdown list. Choose the most relevant option.

Step 4: Fill in the Grievance Details

After selecting the ministry, fill in the required details about your grievance, such as:

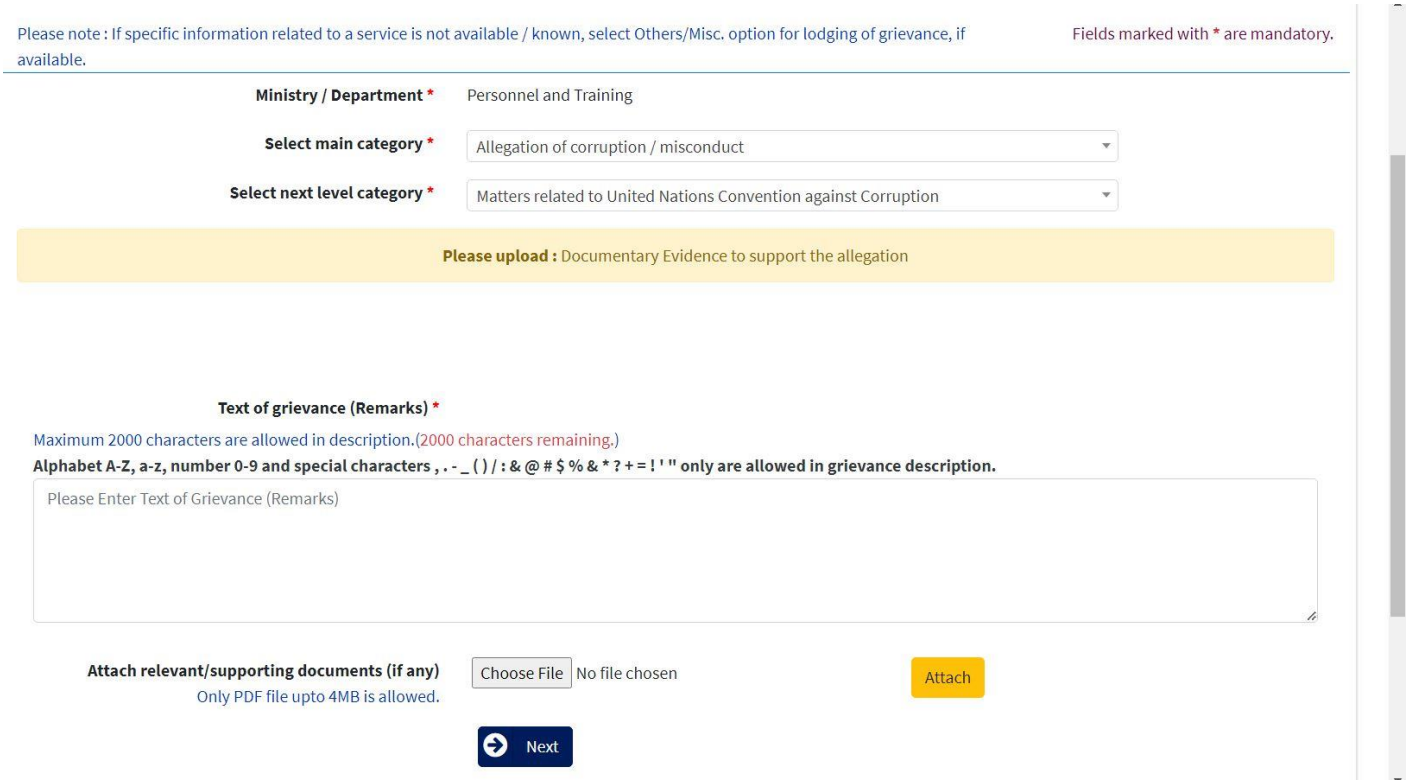
- Subject of the grievance
- Details of the grievance
- Name and contact information
- Attachments (if any)

Step 5: Verify and Submit

Review the entered details for accuracy. If everything is correct, click on the "Submit" button to file your grievance. You will receive a unique registration number for your grievance.

Step 6: Track the Status

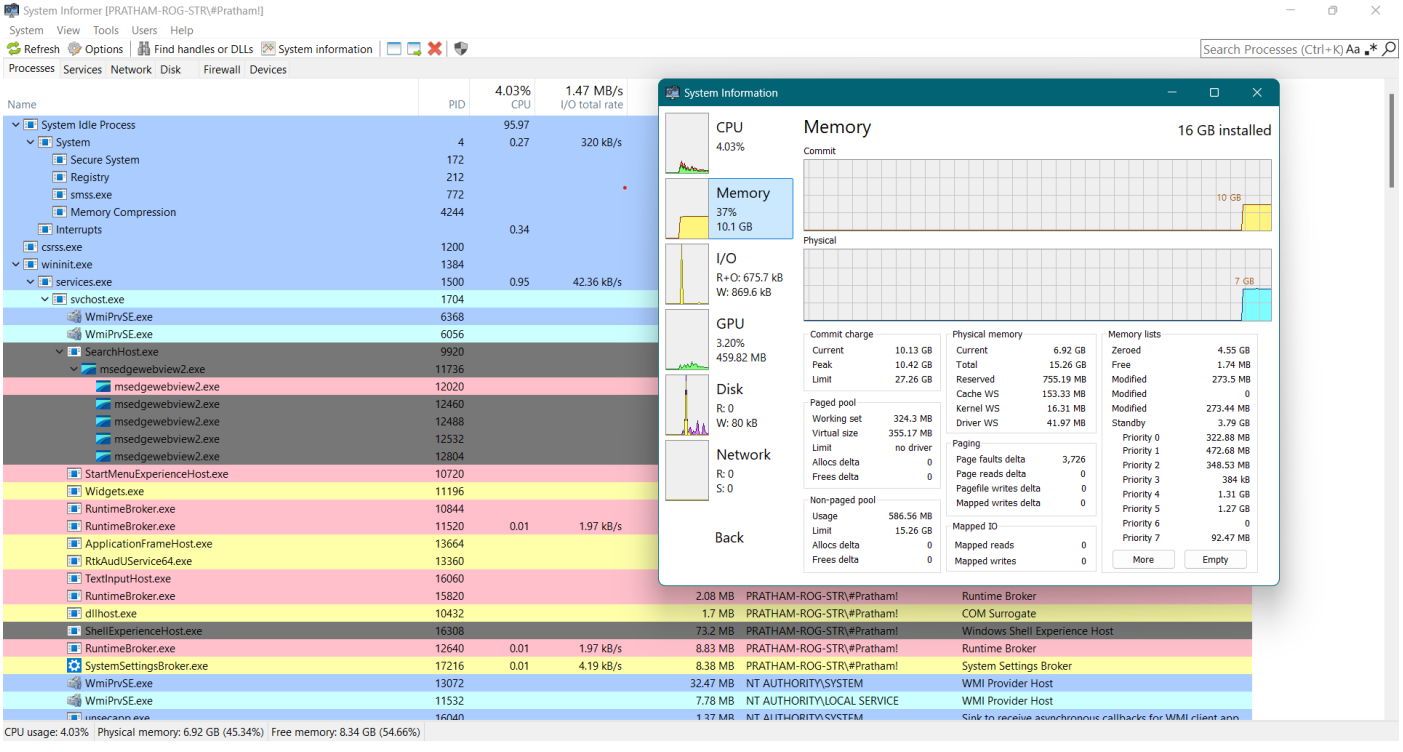
You can track the status of your grievance using the registration number on the "Track Grievance" section of the website. The concerned ministry will process your grievance and provide a resolution.By following these steps, you can easily file a public grievance on the http://pgportal.gov.in website and get assistance from the government authorities.



Assignment 9: Install Hacker Process inside your PC and perform the demonstration.

System Informer is the official successor to Process Hacker and was originally created in 2008 by Wen Jia Liu as an open source alternative to programs such as Windows Task Manager and Sysinternals Process Explorer.

1. Go to System Informer official website. (https://systeminformer.sourceforge.io/)
2. Click on Download System Informer
3. Download setup systeminformer-x.x.xxxx-release-setup.exe
4. Once the download is complete, locate the installer file and double-click it to run it.
5. Follow the on-screen prompts in the installer to complete the installation. Accept the license agreement and choose the installation location.
6. After installation, you can launch System Informer from the Start menu or by searching for it.



Experiment 1: Select any browser and try to secure your browser by following settings:

(i) trusted sited/blocked sites etc.
(ii) by enabling or disabling the cookies.
(iii) use of pop up blocker
(iv) by enabling or disabling scripts
(v) by enabling or disabling scripts
(vi) browsing history
(vii) saving passwords/master password

(i). Trusted Sites/Blocked Sites

- **Google Chrome:**
  - Go to Settings > Privacy and security > Site settings.
  - Under Permissions, you can manage access for different sites, including blocking or allowing access to specific features like camera, location, and more.
  - Scroll down to Content, where you can manage the Trusted sites and Blocked sites.

(ii). Enabling or Disabling Cookies

- **Google Chrome:**
  - Go to Settings > Privacy and security > Cookies and other site data.
  - You can choose to allow all cookies, block third-party cookies, or block all cookies.

(iii). Use of Pop-up Blocker

- **Google Chrome:**
  - Go to Settings > Privacy and security > Site settings.
  - Scroll down to Pop-ups and redirects and toggle it to block or allow pop-ups.

(iv). Enabling or Disabling Scripts

- **Google Chrome:**
  - Go to Settings > Privacy and security > Site settings.
  - Scroll down to JavaScript and toggle it on or off.

(v). Browsing History

- **Google Chrome:**
  - Go to Settings > Privacy and security.
  - Select Clear browsing data to clear history, cookies, and more. You can also set Chrome to clear browsing data every time you close the browser.

(vi). Saving Passwords/Master Password

- **Google Chrome:**
  - Go to Settings > Autofill > Passwords.
  - Toggle Offer to save passwords on or off.
  - To set up a master password, you may need to use an extension like LastPass or Bitwarden.