

# **Secure Browsing with Sandboxie Plus**

**Name: Thirukovela Moulya**

**Roll no: 160123737086**

**Program Name: Assignment-1 of Cyber Security**

**Github Repository: [https://github.com/rishi300101/CyberSecurity\\_SafeBrowsing](https://github.com/rishi300101/CyberSecurity_SafeBrowsing)**

# Secure Browsing with Sandboxie Plus – Final Report

## Project Overview

This project was completed as part of a cybersecurity assignment. The objective was to demonstrate how Sandboxie Plus can be used to provide safe web browsing by isolating the browser in a secure sandbox environment. Instead of blocking suspicious or risky websites, the sandbox allows users to open and interact with them safely, without affecting the actual system.

The project highlights how sandboxing can protect against threats such as malware, phishing links, and unsafe downloads. It reflects real-world use cases where individuals and organizations need a simple yet effective way to ensure safer internet usage.

---

## Technologies & Tools Used

- **Browser Isolation Tool:** Sandboxie Plus
  - **Operating System:** Windows (sandbox host)
  - **Web Browser:** Chrome / Firefox / Edge (run inside sandbox)
  - **File Handling & Recovery:** Sandboxie Quick Recovery feature
  - **Version Control:** Git & GitHub
- 

## System Architecture

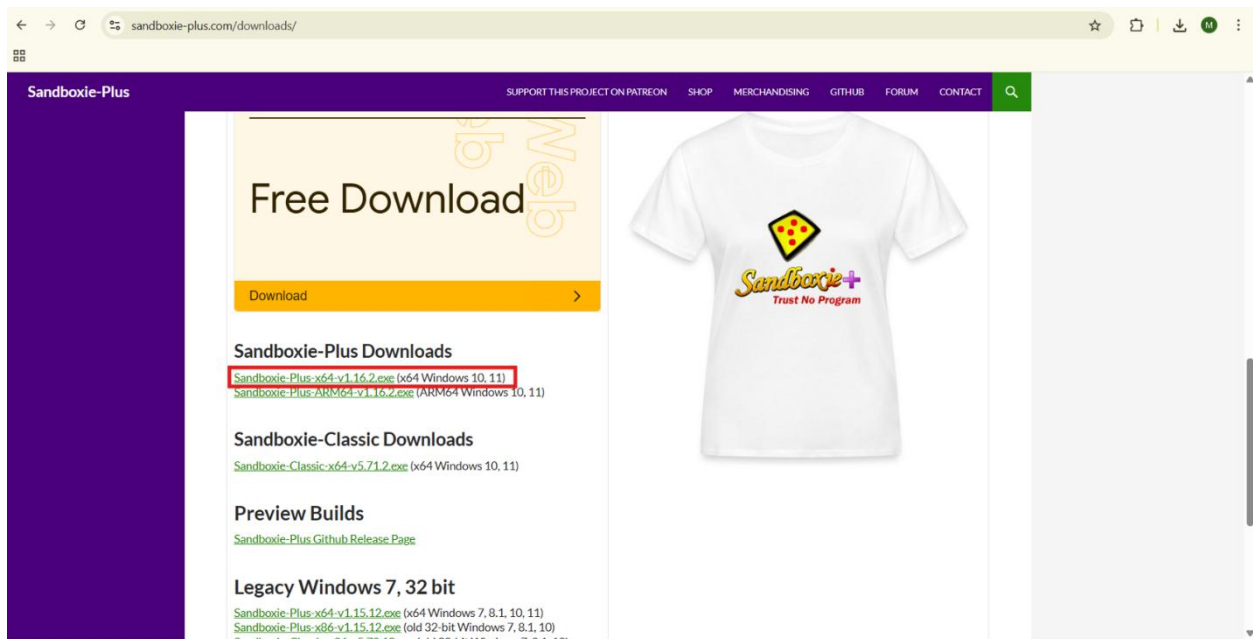
1. The user launches a web browser (Chrome/Firefox/Edge) inside Sandboxie Plus.
2. Any website the user visits runs entirely within the sandboxed environment, isolating it from the host system.
3. Files downloaded from the web are stored in the sandbox container, preventing them from affecting the real system.
4. The user can recover files from the sandbox to the actual system using the **Quick Recovery** feature, if needed.
5. Sandbox settings can restrict internet access or file system access for additional security.
6. Multiple sandboxes can be created simultaneously to isolate different tasks or browsers.
7. Sandbox activity can be monitored in real-time through the Sandboxie control panel.
8. Once the sandbox is deleted, all temporary data (history, cookies, cache, downloaded files) is erased, ensuring the host system remains clean.

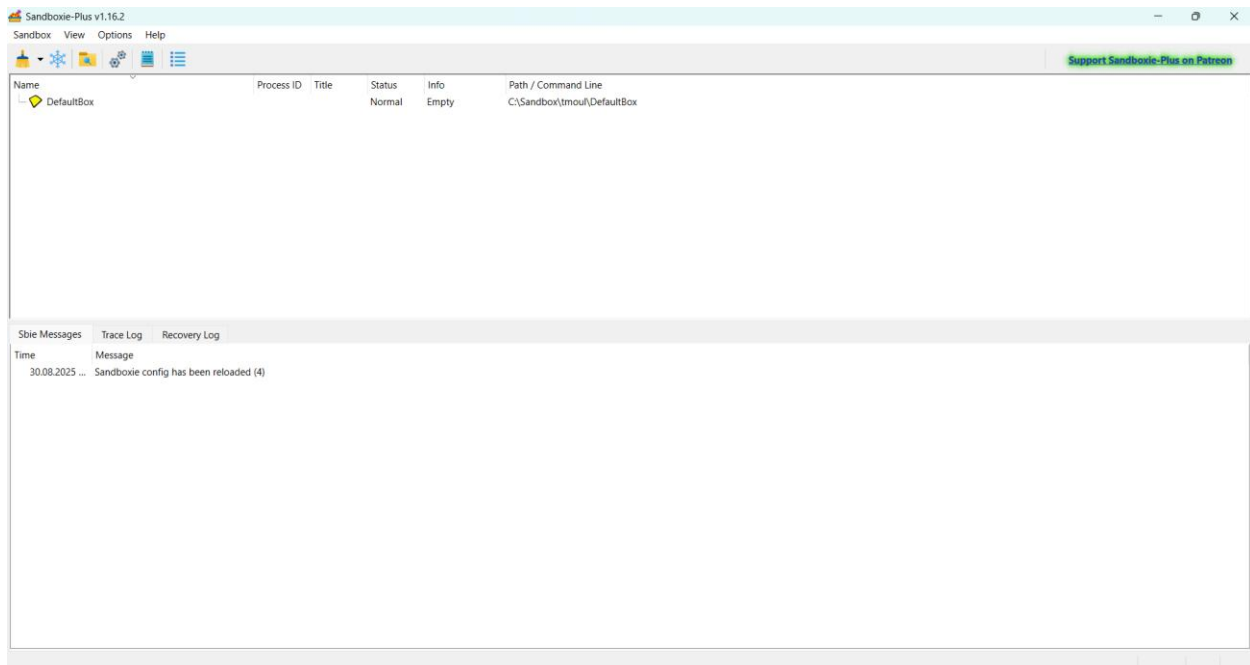
# Security Features

- **Isolation of Browsing Sessions:** All websites and applications run inside the sandbox, preventing any changes to the host system
- **Protected File Downloads:** Files downloaded in the sandbox are contained and cannot affect the real system until explicitly recovered.
- **Temporary Data Containment:** Browser history, cookies, cache, and other data remain inside the sandbox and are erased when the sandbox is deleted.
- **Controlled Program Execution:** Applications can be run with restricted access (internet or file system) to prevent unintended changes.
- **Forced Programs & Sandbox Policies:** Frequently used programs can be configured to always run sandboxed, ensuring consistent security.

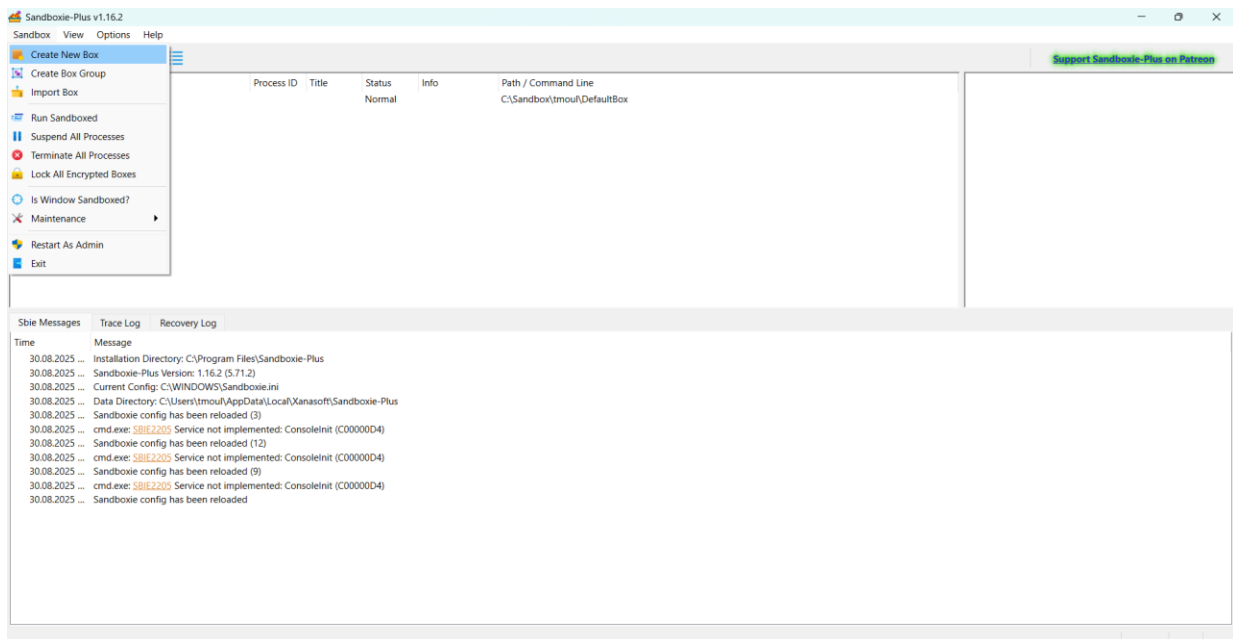
## Screenshots

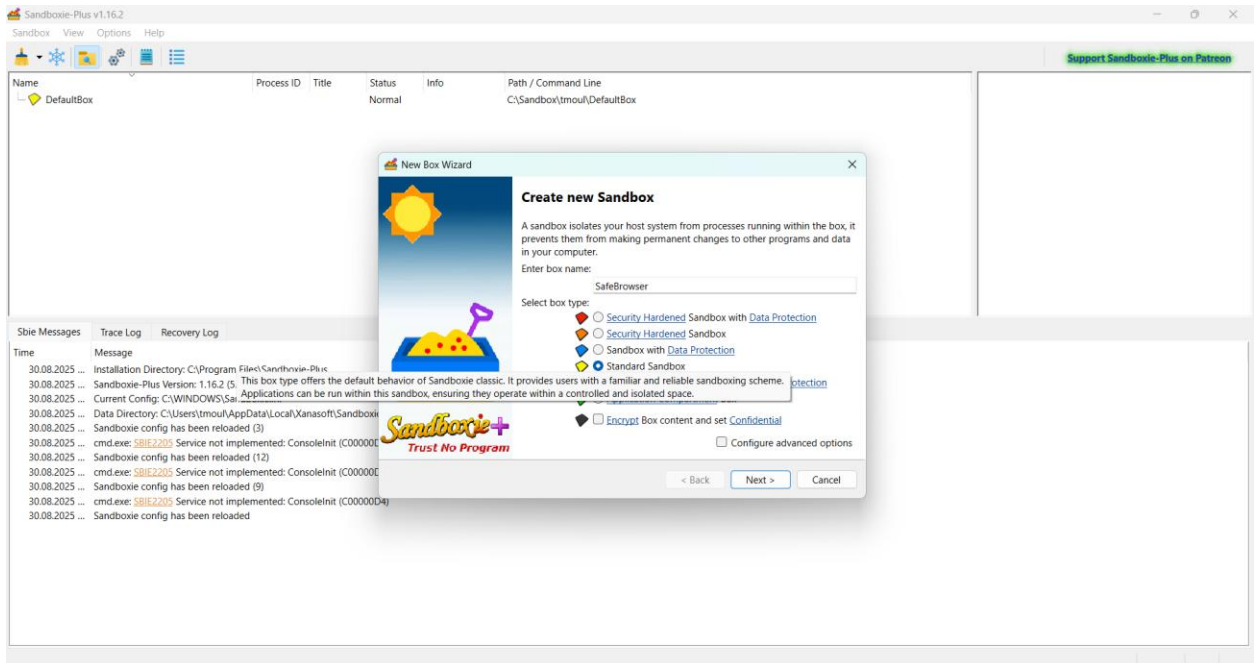
### 1. Installation of Sandboxie plus



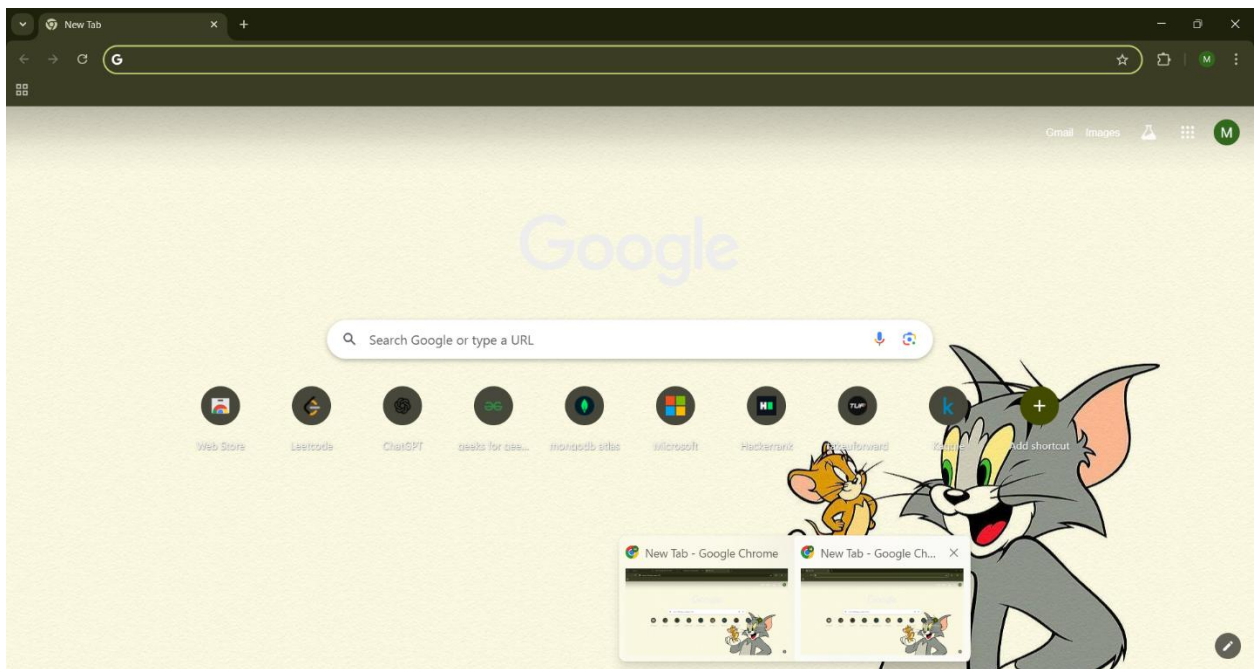


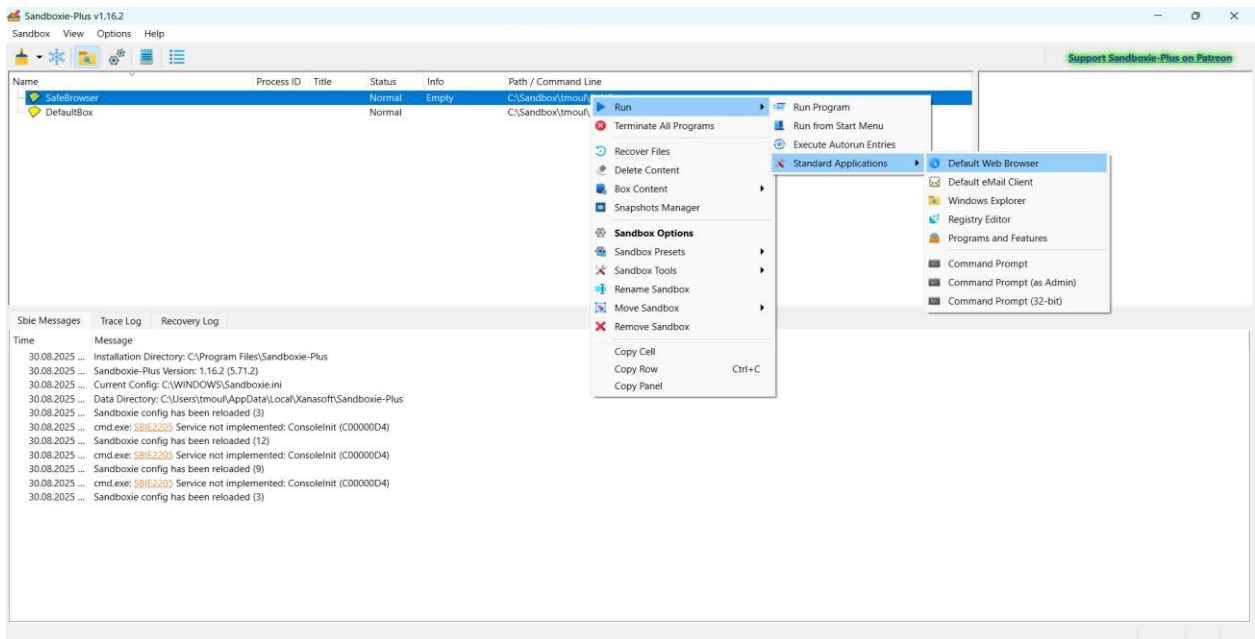
## 2. Create a new Sandbox



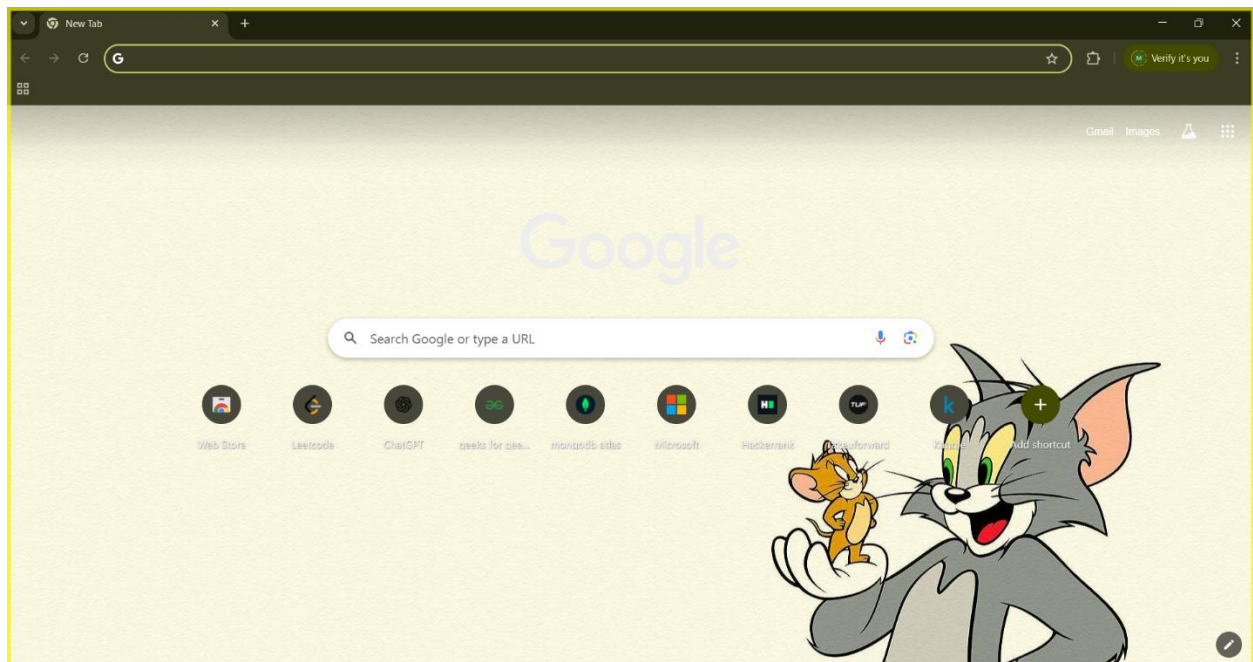


### 3. Default browser





## Sandbox default web browser



CBIT-Registration-Form.pdf

cbt.ac.in/wp-content/uploads/2022/10/CBIT-Registration-Form.pdf

CBIT-Registration-Form.pdf  
118 KB • Done

CBIT-Registration-Form.pdf

1 / 1 | 100% +

**CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY (A)**  
Chaitanya Bharathi P.O., Kolapet (V), Goudpet (M), Hyderabad - 506 075, Telangana State  
Phone No: 040-24193280; Fax No: 040 - 24193278; Website: www.cbit.ac.in

**ACADEMIC & EXAMINATION CELL**

**REGISTRATION FORM**

Date: \_\_\_\_\_

ACADEMIC YEAR: \_\_\_\_\_

1. Name of the Student : \_\_\_\_\_

2. Roll No. : \_\_\_\_\_

3. Name of the Programme : \_\_\_\_\_ Branch \_\_\_\_\_

4. Semester: \_\_\_\_\_ 5. Mobile No.: \_\_\_\_\_ 6. Email ID: \_\_\_\_\_

7. Details of Annual Tuition Fee: (Attach Proofs for Payment)

a) Status of Tuition Fee Payment : \_\_\_\_\_

b) Date of Fee Payment for the Current Academic Year : \_\_\_\_\_

c) Mode of Payment : \_\_\_\_\_

d) Receipt No. with date : \_\_\_\_\_

8. Details of Subjects registering for \_\_\_\_\_ - Semester: \_\_\_\_\_

S. No.	Course Code	Name of the Course	Core / Programme Elective / Open Elective / Project / Seminar	Pursuing through Institute / MOOCs	Remarks

Downloads

Downloads

New Sort View


Name	Date modified	Type	Size
Today			
CBIT-Registration-Form	30-08-2025 19:50	Microsoft Edge PD...	118 KB
Task 3 Future Interns Cyber Security Intern...	30-08-2025 16:38	Microsoft Word D...	245 KB
Sandboxie-Plus-x64-v1.16.2	30-08-2025 11:01	Application	24,122 KB
Earlier this week			
calculator	27-08-2025 11:27	Chrome HTML Do...	3 KB
archive	24-08-2025 14:13	Compressed (zipp...	6,68,805 KB
kaggle	24-08-2025 14:06	JSON Source File	1 KB
Last week			
Thinkovela - Moulva AICTE Certificate	19-08-2025 17:33	Microsoft Edge PD...	342 KB

CBIT-Registration-Form.pdf

cbil.ac.in/wp-content/uploads/2022/10/CBIT-Registration-Form.pdf

CBIT-Registration-Form.pdf

1 / 1 100%



**CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY (A)**  
Chaitanya Bharathi P. O., Kakagudi (V), Gandipet (M), Hyderabad - 500 075, Telangana State  
Phone No: 048-24193286; Fax No: 048 - 24193378; Website: www.cbil.ac.in

**ACADEMIC & EXAMINATION CELL**

**REGISTRATION FORM**

ACADEMIC YEAR: \_\_\_\_\_ Date: \_\_\_\_\_

1. Name of the Student : \_\_\_\_\_

2. Roll No. : \_\_\_\_\_

3. Name of the Programme : \_\_\_\_\_ Branch \_\_\_\_\_

4. Semester: \_\_\_\_\_ 5. Mobile No.: \_\_\_\_\_ 6. Email ID: \_\_\_\_\_

7. Details of Annual Tuition Fee: (Attach Proofs for Payment)

a) Status of Tuition Fee Payment : \_\_\_\_\_

b) Date of Fee Payment for the Current Academic Year : \_\_\_\_\_

c) Mode of Payment : \_\_\_\_\_

d) Receipt No. with date : \_\_\_\_\_

8. Details of Subjects registering for \_\_\_\_\_ Semester:

S. No.	Course Code	Name of the Course	Core / Programme Elective / Open Elective / Project / Seminar	Pursuing through Institute / MOOCs	Remarks

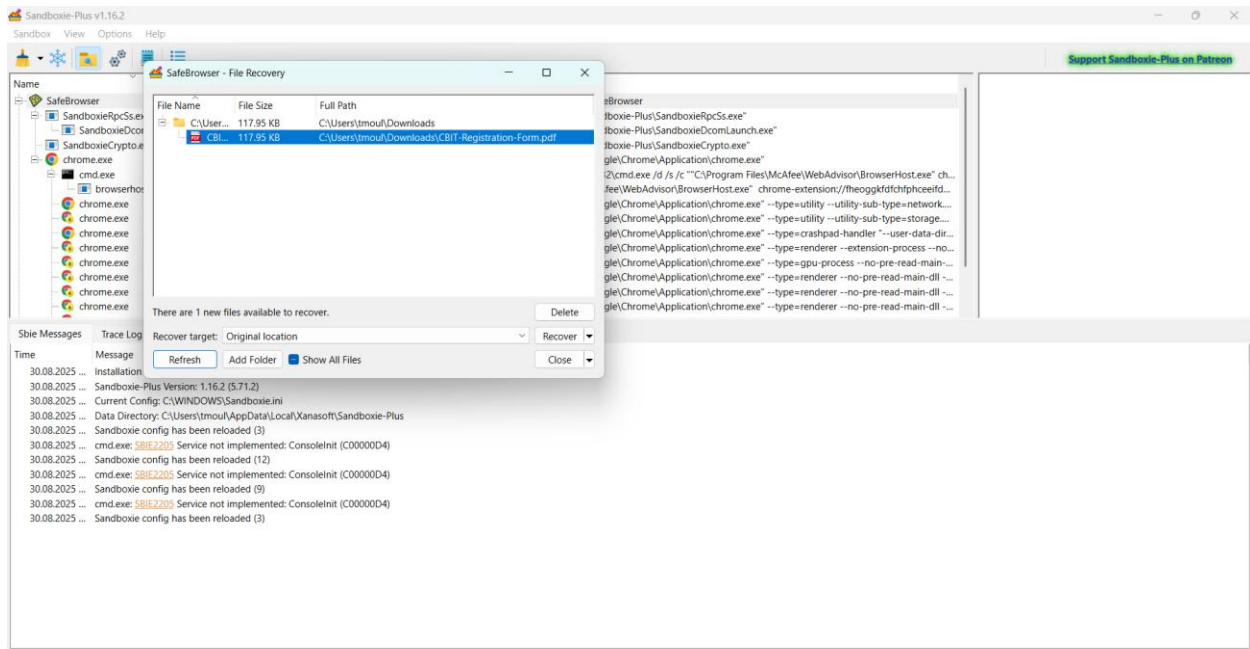
Downloads

Search Downloads

Name	Date modified	Type	Size
Today			
Task 3 Future Interns Cyber Security Intern...	30-08-2025 16:38	Microsoft Word D...	245 KB
Sandbox-Plex-v54-v1.15.2	30-08-2025 11:01	Application	24,122 KB
Earlier this week			
calculator	27-08-2025 11:27	Chrome HTML Do...	3 KB
archive	24-08-2025 14:13	Compressed (zip...	668,805 KB
kaaggle	24-08-2025 14:06	JSON Source File	1 KB
Last week			
Thirukovela Moujya_AICTE_Certificate	19-08-2025 17:33	Microsoft Edge PD...	342 KB
invite	18-08-2025 18:47	iCalendar File	6 KB
chess	17-08-2025 17:42	Chrome HTML Do...	2 KB
styles	17-08-2025 17:40	CSS Source File	1 KB
index	17-08-2025 17:39	Chrome HTML Do...	2 KB
Login_form	17-08-2025 13:40	Chrome HTML Do...	5 KB
register	17-08-2025 13:39	Chrome HTML Do...	3 KB
Earlier this month			
WebEx_mmc_infyevents_infyevents.webex...	12-08-2025 17:04	Application	467 KB
treas_CNN (1)	04-08-2025 20:54	Jupyter Source File	1,425 KB
Week_3_Project_PPT_Template1 (1)	04-08-2025 19:55	Microsoft PowerPo...	1,018 KB
LMS_Process_Document	01-08-2025 22:50	Microsoft Edge PD...	1,182 KB
Weekly_Milestones_and_Project_Submissi...	01-08-2025 22:49	Microsoft Edge PD...	632 KB
Week_3_Project_PPT_Template1	01-08-2025 22:46	Microsoft PowerPo...	1,018 KB

93 items





## Testing & Results

- Verified that files downloaded through the sandboxed browser were stored only in the sandbox container, not on the host system
- Tested the **Quick Recovery** feature to successfully move selected files from the sandbox to the real system.
- Confirmed that browser history, cookies, and cache created during the sandbox session were erased after deleting the sandbox.
- Validated that running other applications (e.g., Notepad) inside the sandbox did not affect the host system.

**Result:** The system successfully isolated all browsing and application activity inside the sandbox. Downloaded files and temporary data remained contained, and the host system stayed clean and unaffected after sandbox deletion.

---

## Deliverables

- GitHub Repository containing the walkthrough video and the output screenshots
- Walkthrough video (uploaded on GitHub) demonstrating sandboxed browsing, file download & recovery, data isolation, and sandbox deletion.
- Final Security Report (this document) describing system architecture, security features, testing, and results.

---

## Learning Outcomes

- Gained practical understanding of sandboxing technology and its role in cybersecurity.
- Learned how to run web browsers and applications safely in an isolated environment.
- Understood the process of file download, recovery, and containment within a sandbox.
- Experienced how browser data (history, cache, cookies) can be isolated and erased to maintain system cleanliness.

---

## Conclusion

This assignment successfully demonstrates the use of Sandboxie Plus as a browser isolation tool. By running web browsers and applications in a sandboxed environment, it was shown that risky activities such as visiting unknown websites or downloading files can be performed safely without impacting the host system. Features like file recovery, data isolation, and sandbox deletion highlight the practicality of sandboxing for everyday security needs. Overall, this assignment provided hands-on experience with a real-world security tool and improved understanding of how sandboxing helps protect against online threats.