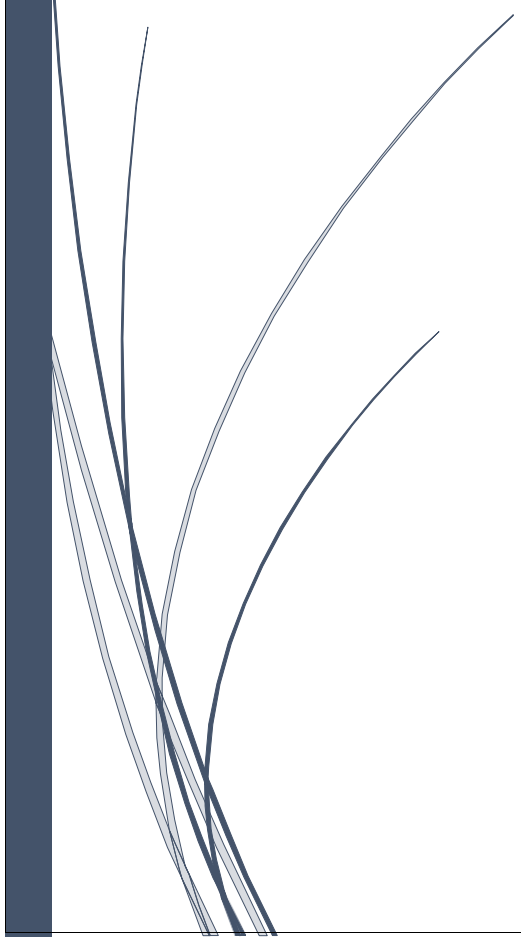
06/10/2023

USB Physical Ports Security Using Python



Supraja Technologies

COMPANY PROFILE

Dear Sir/Madam,

We are pleased to inform you that Supraja Technologies is offering Trainings in various domains especially like

- **Ethical Hacking & Cyber Security**
- **Cyber Forensics**
- **IOT Security**

Training plays an important role in the curriculum of a student, it plays very crucial role in upcoming career aspect of the students as it provides them the gist of the industry in which they want to opt for. There are too many segments or sectors where students can go for. However, there is a pre requisite of having appropriate skill set and thorough knowledge about the relevant technology which can help them to enter into the industry. Due to an increase in the number of skilled unemployed and cut throat competition in the job market today, industry demands quiet efficient and more skilled manpower. And this competition has created the demand for industrial exposure and industry based support to the student in their course curriculum itself.

Supraja Technologies is continuously putting its efforts to fulfil this demand and supply gap between the industry and institutes with the help of different types of course content for students. Our extensive R&D based course module helps students out in understanding these new and upcoming technologies as per industry norms and impart practical exposure in them so that they can get ready for tomorrow and make their career in respective segment itself.

COMPANY INTRODUCTION:

Supraja Technologies is a leading Knowledge and Technical Solutions Provider and pioneer leader in IT industry, is operating based out of Vijayawada, Guntur, Visakhapatnam, Hyderabad and Bangalore.

R&D at Supraja

With a 24X7 work in Research & Development, experts at Supraja Technologies work under :

- **Cyber Security Cell**

About Supraja Technologies:

Supraja Technologies (a unit of CHSMRLSS Technologies Pvt. Ltd.) with its foundation pillars as Innovation, Information and Intelligence is exploring indefinitely as a **Technology Service Provider** and as a **Training Organization** as well.

You may visit us at :
www.suprajatechnologies.com

The multi domains of trainings which Supraja Technologies operate include the following :

- **Workshops & Hackathons**
  - Engineering Colleges
  - Schools
  - Corporate (Private & Govt)

- **Classroom Trainings Cum Certification Courses**
  - Summer Training (30-45 Days)
  - Winter Training (10 - 15 Days)
  - Weekend Training (2 Days)
  - 1 Month / 3 Months / 6 Months Courses

- **On-site Trainings**
  - College Summer Training (15 Days, 30 Days, 45 Days & 60 Days)
  - School Summer Camp (15 Days & 30 Days)
  - Govt Agencies, Police Academies, Corporates

- **Cloud Campus**
  - (Distance Learning Program) *Coming Soon

- **Internships**
  - Internship for Engineering Students (15 Days, 30 Days, 45 Days & 60 Days)
  - Internship for Graduates (15 Days, 30 Days, 45 Days & 60 Days)

- **Lab Setup**
  - Cyber Lab

Why Supraja Technologies:

Be it Training or a workshop, the course content is always from R&D Cell of Supraja.

- A proven track record of delivering quality services.
- **68,500+** Students trained by our trainers till date.
- Training Partners of recognized institutions.
- Trainers with excellent research aptitude and teaching pedagogy illustrate their findings through **practical demonstrations** during their sessions.
- Easy to learn and **hands-on sessions** are given, with additional benefits of Study Material, Tool kit DVD's and immediate query handling.
- Self-Prepared **Cyber Security Cell.**
- Supraja Technologies has the best, experienced and highly **skilled bunch of R&D Engineers & Trainers.**
- We provide training in Innovating and Trending Technologies to Govt. Officials, Corporate Houses and Colleges.

✓ Something we are proud of :

1. Supraja Technologies CEO Mr.Santosh Chaluvadi is an Alumni of Potti Sriramulu Chalavadi Mallikharjuna Rao College of Engineering and Technology, Vijayawada.

With our CEO this college conducted/organised a 50 hours Nonstop Marathon Training Workshop on Ethical Hacking & Cyber Security for which this respective college and our CEO both holds their name in **"LIMCA BOOK OF RECORDS 2017"**

2. We are very happy to inform you all that our company, Supraja Technologies has been shortlisted for **"Top 50 Tech Companies" award 2019**, conferred at InterCon - Dubai, UAE.

   Supraja Technologies is one out of thousands companies that were initially screened by InterCon team of 45+ research analysts over a period of three months and the final shortlist includes 150+ firms and we are very proud to inform you all that our company Supraja Technologies also happens to be a part of the same.

✓ Life changing solution/service :

After working on R&D for around 2 years, finally in the mid 2019 we have successfully developed a service/solution of various techniques and strategies for the Film Industry through which he can kill piracy of any film in online up to 25% right now. This betaservice is being appreciated & adopted by various Tollywood Film Industry Producers & Hero's to safeguard their film from piracy in online and to gain more profits.

By the end of 20230 our vision is to rollout a complete full packed service/solution where we can kill piracy entirely 100% everywhere in online for sure.

Apprecation :

Received a great appreciation from our 1st Tollywood Film Industry client Mr.Saptagiri for providing our Anti-Piracy betaservice for his film VAJRA KAVACHADARA GOVINDA

Thanks & Regards,

SANTOSH CHALUVADI
Founder & CEO
+91 – 95500 55338 (M), +91 – 79013 36873 (O)
santosh@suprajatechnologies.com
www.suprajatechnologies.com

Santosh Chaluvadi

Founder & CEO
Supraja Technologies

He is a 27-year-old entrepreneur, one of the India's efficient Cyber Security Analyst and also he is an expert Digital Marketer as well. He is a digital marketer by profession and security enthusiast by passion. He primarily focuses on content building, testing and monetization of blogs. He has successfully developed many websites and done the security testing himself to ensure that the user's data is in safe hands and their privacy is protected. He is very active on social media and shares lot of tech stuff with his followers. The young student hacker has solved many issues with the vulnerabilities present in various websites and databases, given a solution in clearing the loopholes in order to protect the data to be leaked from the databases. Besides Ethical Hacking & Cyber Security, he also has a passion in Blogging & Digital Marketing.

While pursuing his engineering itself, he has trained many young generation people/students of more than 3500+ from various parts across Andhra Pradesh through his workshops, seminars, courses in Cyber Security and this makes him one of the youngest student trainers in India.

At the age of 20 he conducted his first workshop on Blogging & Ethical Hacking which was the beginning to his success in this field and right now he has handful of workshops to train students, government and corporate organizations as well in Andhra Pradesh & Telangana. He is the only student trainer who started conducting workshop for his peers and professors.

❖ Records, Appreciations, Awards & Recognitions etc at a glance :

- ✓ Holds a National Record in **Limca Book of Records – 2017**
- ✓ Steering Committee Member for **United Conference on Cyber Space (UNITEDCON 2020)**
- ✓ Ex-Associate Member for **National Cyber Safety and Security Standards (NCSSS)**
- ✓ Awarded as a **"Karmaveer Chakra - 2019"**, on 12th October 2019 at IIT Delhi, which was instituted by iCONGO in partnership with the United Nations
- ✓ Awarded as a **"Social Media Influencer - 2019"**, on 30th June 2019 by Jignasa in association with Government of Andhra Pradesh
- ✓ Nominated for **INDIA 500 CEO AWARD 2019**
- ✓ Invited & **Interviewed by ETV Andhra Pradesh news channel** on 27th July, 2019 for a Special Story Interview on "Spy Apps"
- ✓ **Appreciated by Mr.Sridhar Garu, Sub-Inspector of Police at Central Crime Branch, Vijayawada** on 23rd October, 2018 for exclusively training him on Special Investigation Course, which will help him to solve the cases easily
- ✓ **Received a great appreciation from our 1st Tollywood Film Industry client Mr.Saptagiri,** for providing **Anti-Piracy betaservice** for his movie VAJRA KAVACHADARA GOVINDA

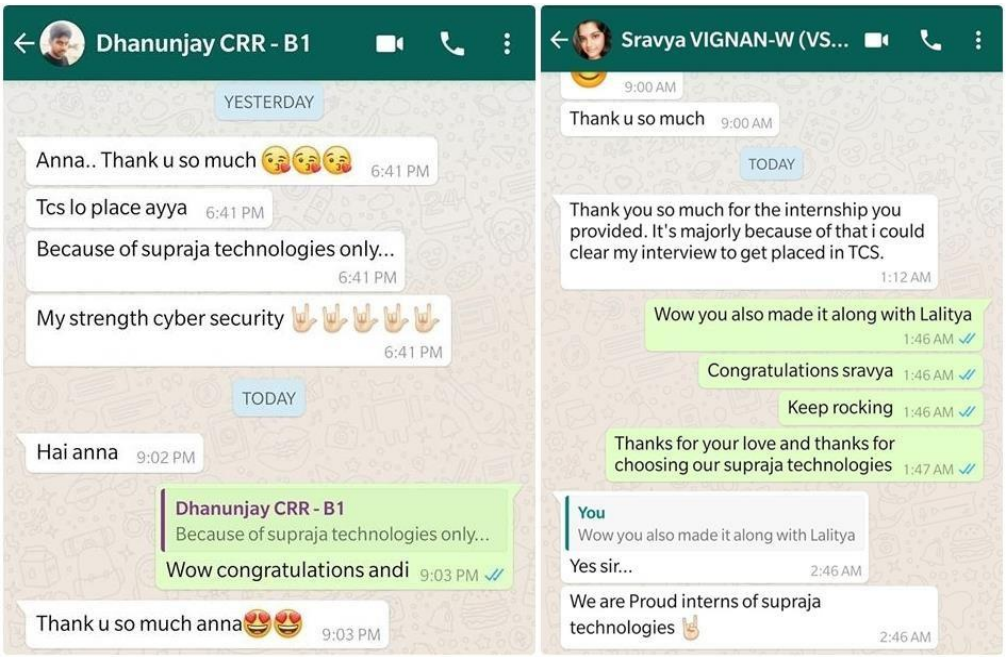
Some Glimpses of our Journey

Mr.Santosh Chaluvadi – CEO, Supraja Technologies
Giving hands-on Cyber Security training workshop to the CSE students
at IIT Kharagpur

Mr.Santosh Chaluvadi – CEO, Supraja Technologies was
Invited & Interviewed by ETV Andhra Pradesh news channel on 27th July, 2019
for a Special Story Interview on "Spy Apps"

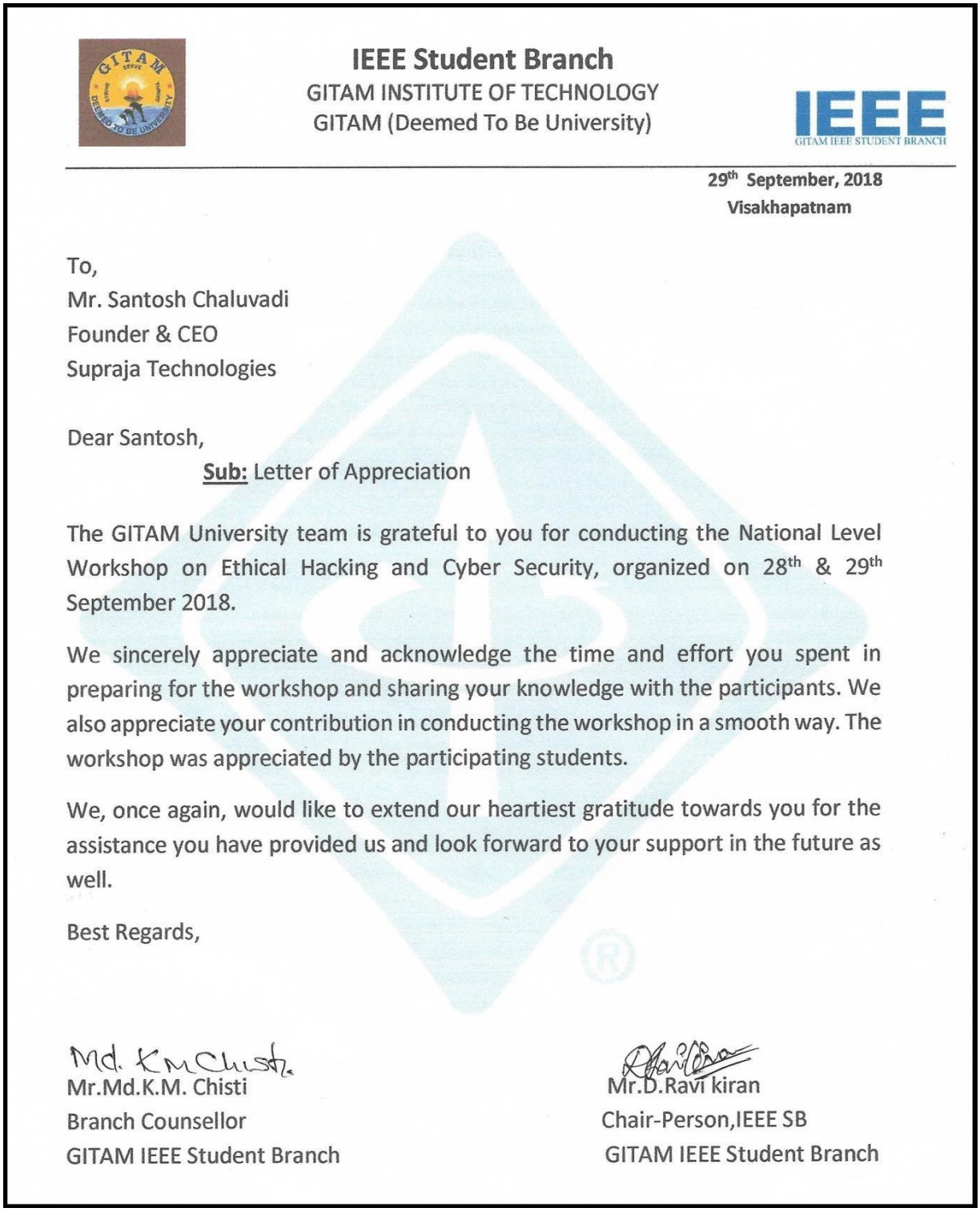
Mr.Santosh Chaluvadi – CEO, Supraja Technologies
Giving Cyber Security training to the students at IIIT Nuzvid

SUPRAJA TECHNOLOGIES
(a unit of CHSMRLSS Technologies Pvt. Ltd.)
An MSME & ISO 9001:2015 Certified Company
Regd. & Head Office : Door No. 11-9-18, 1st Floor, Majjivari Street, Kothapeta, Vijayawada – 520001.
contact@suprajatechnologies.com | www.suprajatechnologies.com | +91 - 9550055338



In Pictures : Success stories of some of our Internship students of 2019

1. Mr. K Dhanunjay of Sir C R Reddy College Of Engineering, Eluru
2. Ms. Sravya Susarla of Vignan's Institute of Management & Tech for Women, Vizag
3. Mr. Arbaaz Dilkush Mohammad of Srinivasa Ramanujan Institute of Tech, Anantapur



IEEE Student Branch
GITAM INSTITUTE OF TECHNOLOGY
GITAM (Deemed To Be University)

IEEE
GITAM IEEE STUDENT BRANCH

29th September, 2018
Visakhapatnam

To,
Mr. Santosh Chaluvadi
Founder & CEO
Supraja Technologies

Dear Santosh,

Sub: Letter of Appreciation

The GITAM University team is grateful to you for conducting the National Level Workshop on Ethical Hacking and Cyber Security, organized on 28th & 29th September 2018.

We sincerely appreciate and acknowledge the time and effort you spent in preparing for the workshop and sharing your knowledge with the participants. We also appreciate your contribution in conducting the workshop in a smooth way. The workshop was appreciated by the participating students.

We, once again, would like to extend our heartiest gratitude towards you for the assistance you have provided us and look forward to your support in the future as well.

Best Regards,

Md. K.M. Chisti
Mr.Md.K.M. Chisti
Branch Counsellor
GITAM IEEE Student Branch

Mr.D.Ravi kiran
Chair-Person,IEEE SB
GITAM IEEE Student Branch

Pic Credits : Appreciation from GITAM University, Visakhapatnam

Santhosh gets award for service in cyber security

HANS NEWS SERVICE

Vijayawada: Supraja Technologies head Ch Santhosh received 'Karmaveer Chakra Award-2019' from Mahender Singh Seva Foundation founder Gurlin Kohli. The award was presented by i-Congo organisation to Supraja Technologies for their service in cyber security at a programme organised at the IIT Delhi campus on October 12.

Santhosh said that he completed his computer science engineering from Potti Sriramulu Engineering College and started Supraja Technologies. He said that about 1,500 experts and talented people have been selected across the country and a few were given awards based on their service in the field of technology.

Potti Sriramulu College Chairman Ch Mallikarjuna Rao Secretary R Subba Rao, Treasurer K Venkateswara Rao principal Dr K Nageswara Rao and others congratulated Santhosh on his achievement.

Santhosh receiving Karmaveer Chakra Award 2019 at IIT Delhi

THE HANS INDIA Mon, 14 October 2019
https://epaper.thehansindia.com/c/44641990

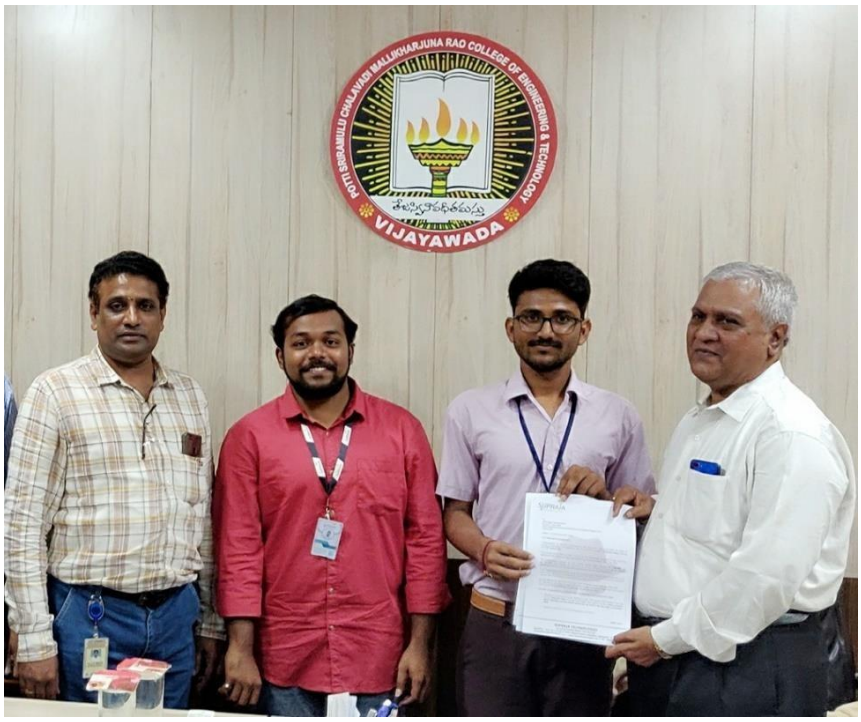
Mr. Santosh Chaluvadi, CEO – Supraja Technologies was featured in THE HANS INDIA newspaper regarding his recently received **"Karmaveer Chakra Award 2019"** on October 12th at IIT Delhi, which was instituted by iCONGO in partnership with the United Nations

Mr.Santosh Chaluvadi – CEO, Supraja Technologies gave hands-on Cyber Security training for the students from Dept. of IT at G.Narayanamma Institute of Technology & Science, Hyderabad

Mr.Santosh Chaluvadi – CEO, Supraja Technologies was awarded as a **"Social Media Influencer 2019"** in recognition of his remarkable achievements in the social media as a part of First International Social Media Festival on 30th June 2019 by Jignasa in association with Government of Andhra Pradesh

Mr.Santosh Chaluvadi – CEO, Supraja Technologies
Giving awareness on the latest cyber-attacks to the CSE & IT students at Vasireddy Venkatadri Institute of Technology, Guntur

On 23rd October 2018 Mr.Santosh Chaluvadi, CEO - Supraja Technologies and Mr.Krishna Chaitanya, CTO - Supraja Technologies has successfully completed delivering Special Investigation Course training in Cyber Security to Mr.Sridhar Garu, Sub-Inspector of Police at Central Crime Branch, Vijayawada which will help him to solve the cases easily



11th March 2019 is a special day for Mr.Santosh Chaluvadi, CEO - Supraja Technologies as he hired a candidate with a salary package of 4.8 LPA from the same college where he studied his engineering ie., Potti Sriramulu Chalavadi Mallikarjunarao College of Engineering and Technology, Vijayawada

ETV Andhra Pradesh News Channel interviewed Mr.Santosh Chaluvadi, CEO - Supraja Technologies for his achievements in the domain of Cyber Security & Digital Marketing

Mr.Santosh Chaluvadi – CEO, Supraja Technologies with some of the Internship selected candidates of Supraja Technologies from the Department of IT, Institute of Aeronautical Engineering, Hyderabad

Mr.Santosh Chaluvadi – CEO, Supraja Technologies
was felicitated by the department of CSE at St.Mary's Group Of Institutions, Guntur

Supraja Technologies was invited by Indian Air Force (Air Wing NCC) to deliver a session on Latest Cyber Crimes & Awareness for the NCC cadets, staff and officers on 4th July, 2019

Supraja Technologies – CEO, CTO & CMO with
Indian Air Force (Air Wing NCC) Group Captain Sandeep Gupta.
We thank Mr.Sandeep Gupta for inviting us to deliver a session on Latest Cyber Crimes & Awareness for the Indian Air Force (Air Wing NCC) cadets, staff & officers

On 7th March 2019 Mr.Santosh Chaluvadi, CEO - Supraja Technologies has hired 4 candidates who has successfully completed their Internship in our Supraja Technologies and finally for their top class performance we appreciated them by offering a pre-placement opportunity in our company

In Picture : Mr.Santosh Chaluvadi, CEO - Supraja Technologies along with the Professor, HOD of Computer Science & Engineering and Chairperson, Board of Studies at GITAM University Visakhapatnam, Mr.Thammi Reddy giving away the pre-placement offer letters to the shortlisted candidates of Supraja Technologies

Mr.Santosh Chaluvadi along with his Team / Trainers has conducted / organised Workshops, Seminars and Courses on Cyber Security / Ethical Hacking at the following educational institutions and organizations:

- IIT Kharagpur, hosted by AIESEC
- PES University, Bangalore
- GITAM University, Vizag
- CBIT, Hyderabad
- IIIT, Nuzvid
- 2019 Latest Cyber Crimes & Awareness Sessions for the NCC cadets, staff & officers of Indian Air Force (Air Wing NCC)
- Sainik School Korukonda – Under Ministry of Defence
- Vasavi College of Engineering, Hyderabad
- University College of Engineering, Osmania University – Hyderabad
- G. Narayanamma Institute of Technology and Science, Hyderabad
- Institute of Aeronautical Engineering, Hyderabad
- VNR Vignana Jyothi Institute of Engineering & Technology, Hyderabad
- Vardhaman College Of Engineering, Hyderabad
- Sreenidhi Institute Of Science & Technology, Hyderabad
- Stanley College of Engineering and Technology for Women, Hyderabad
- University College of Engineering, JNTUK – Vizianagaram
- MVGR College of Engineering, Vizianagaram
- Satya Institute of Technology and Management, Vizianagaram
- Andhra Loyola Engineering College, Vijayawada
- NRI Institute of Technology, Guntur
- St. Mary's Group Of Institutions, Guntur
- Sir C R Reddy College Of Engineering, Eluru
- Eluru College Of Engineering & Technology, Eluru
- Viswanadha Institute of Technology and Management, Vizag
- Raghu Engineering College, Vizag
- Chaitanya Engineering College, Vizag
- Avanthi Institute Of Engineering & Technology, Vizag
- Bomma Institute Of Technology & Science, Khammam
- RISE Group of Institutions, Ongole

- Lakkireddy Balireddy College of Engineering, Mylavaram
- DNR Engineering College, Bhimavaram
- Grandhi Varalakshmi Venkata Rao Institute of Technology, Bhimavaram

and many more workshops, corporate trainings, seminars, faculty development programs, one-one sessions, online trainings etc...

Thanks & Regards,

SANTOSH CHALUVADI
Founder & CEO
+91 – 95500 55338 (M), +91 – 79013 36873 (O)
santosh@suprajatechnologies.com
www.suprajatechnologies.com

SUPRAJA TECHNOLOGIES – KEY TRAINER

Krishna Chaitanya

- **Chief Technology Officer**
- **Head - IT Security**
- **Head - Cyber Forensics Investigation**
- **Chief Trainer at Supraja Technologies**

He is a 27 year old passionate, goal-oriented IT professional in Computer Digital Forensics & Ethical Hacking. He is an expert in Vulnerability Assessment and Penetration Testing (VAPT). He holds a responsible and challenging position with a turbulent and dynamic professional development and where he can best utilize his knowledge and skills. He has been assisting for Telangana State Police Academy and various Government Department Officials, Private sector Officials across India.

WHAT I DO : (DIGITAL FORENSICS)

The Advanced Digital Forensics focuses on the entire investigative process, from the very beginning through the conclusion and determination of who did it. Adequate knowledge on Digital Forensics which can drive me to investigate typical Cyber Crimes. Handling incident response and perform analysis to trace out the foot prints.

- Develop an investigative process for the digital forensic investigation
- Understanding methods of focusing investigations through analysis of multiple evidence sources
- Effectively prepare for incident response of both victim and suspect systems, including understanding the importance of network reconnaissance and network traffic analysis
- Identify sources of evidentiary value in various evidence sources including network logs, network traffic, volatile data and through disk forensics
- Identify common areas of malicious software activity and characteristics of various types of malicious software files
- Confidently perform live response in intrusion investigation scenarios
- Recovering data from damaged or erased hard drives.
- Writing, reviewing investigative reports & gathering, maintaining evidences

- Working closely with other police officers and detectives
- Imaging & Hashing

WHAT I DO : (VA&PT)

Analyses and assesses vulnerabilities in the infrastructure (applications & networks), investigates the available tools and countermeasures to remedy the detected vulnerabilities, and recommends solutions and best practices. Analyses and assesses damage to the data/infrastructure as a result of security incidents, examines available recovery tools and processes, and recommends solutions. Tests for compliance with security policies and procedures may assist in the creation, implementation and/or management of security solutions.

TRAINING :

Now-a-days the demand for Computer Digital Forensics & Ethical Hackers has increased. I used to give training for corporate companies, schools and college students. I used to conduct seminars and workshops for the same. I possess strong background knowledge of Ethical Hacking, Computer Digital Forensics, Networking, Web Applications, Current security protocols for popular operating environments etc.

CERTIFICATIONS, HONORS, APPRECIATIONS, AWARDS & RECOGNITIONS:

- CPEH : Certified Professional Ethical Hacker
- CPTE : Certified Penetration Testing Engineer
- CHFI : Certified Hacking Forensics Investigator
- RHCE : Red Hat Certified Engineer
- Worked as a core member for National Information Security Summit 2017
- Appreciation from E-HACK
- Appreciation Certification from National Cyber Safety & Security Standards
- Appreciation for finding out Vulnerabilities in websites like Sony, Intel etc
- Appreciation from Telangana State Police Academy for training some of the department officials on various Cyber Attacks
- Honoured & Appreciated from Honourable Member of Parliament and Telangana

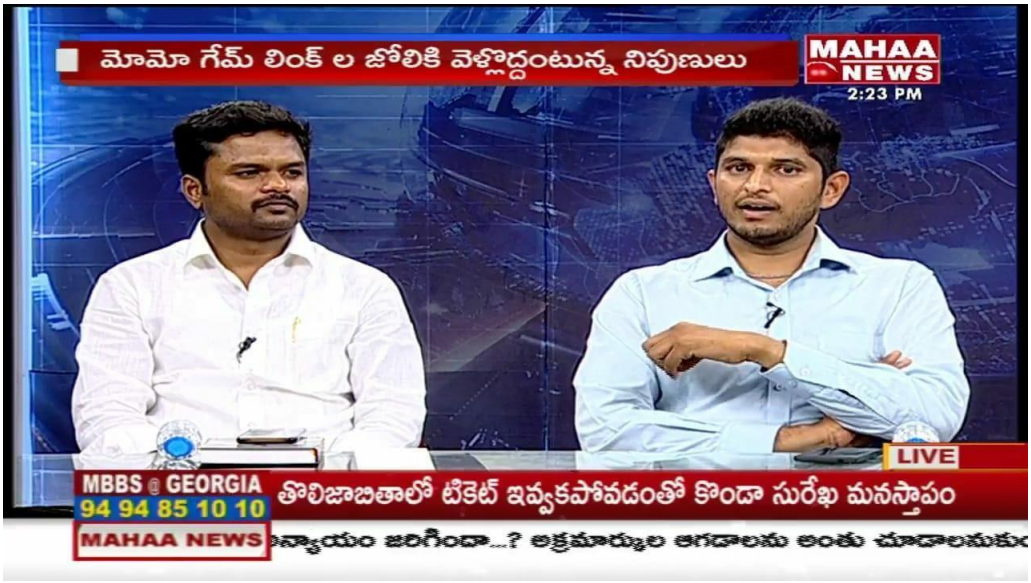
Rashtra Samithi party member Smt. Kalvakuntla Kavitha Garu

- Appreciated by various Universities, College Managements, Organizations and Technocrats
- Invited by Mahaa News channel on Sept 8, 2018 for a Live Debate on Momo Challenge

Mr.Krishna Chaitanya – CTO, Supraja Technologies
Giving training to the department staff at Telangana State Police Academy

Mr.Krishna Chaitanya – CTO, Supraja Technologies
With some of the department officials at Telangana State Police Academy

Mr.Krishna Chaitanya – CTO, Supraja Technologies
Honoured & Appreciated from Honourable Member of Parliament and Telangana Rashtra Samithi party member Smt. Kalvakuntla Kavitha Garu



Mr. Krishna Chaitanya – CTO, Supraja Technologies
Invited by Mahaa News channel @ Sept 8, 2018 for Live Debate on Momo Challenge

INDEX

USB Physical Ports Security Using Python

Abstract:

The project aimed to develop a Graphical User Interface (GUI) application for user authentication and USB port control. The system would allow users to enter their username and password, and upon successful validation, it would lock or unlock the USB ports. Ensure the security of your sensitive data with our USB blocking software. Prevent confidential information from being copied to unauthorized removable storage devices and minimize the risk of data loss and data leaks. Get protection against the spread of USB malware and potential data breaches with an effective USB port lock software. Enforce USB blocking policies easily and prevent any malicious activity that might otherwise take place around your USB ports.

Introduction:

In today's digital era, ensuring the security of sensitive data is of paramount importance. Unauthorized access to systems and data via USB ports is a potential security risk. This project aimed to mitigate this risk by implementing a secure user authentication mechanism and controlling the USB ports based on user credentials.

USB (Universal Serial Bus) ports are commonly found on computers and other electronic devices, allowing users to connect various peripheral devices such as keyboards, mice, printers, and external storage devices. While USB ports offer convenience and ease of use, they can also pose security risks by enabling unauthorized data transfer or introducing malicious software.

USB port lock and unlock functionality is designed to address these security concerns. It provides a means to control access to USB ports, allowing users or administrators to selectively enable or disable their functionality based on specific requirements or security policies.

The purpose of USB port lock and unlock is to prevent unauthorized data transfer, protect sensitive information, and mitigate potential threats. By locking USB ports, organizations can safeguard against data theft, prevent malware infections, and maintain control over the usage of peripheral devices within their network or system.

When USB ports are locked, they become non-functional, thereby prohibiting any data transfer to or from connected USB devices. This prevents unauthorized individuals from connecting external storage devices to extract data or introduce malicious software. USB port lock and unlock mechanisms can be implemented through software or hardware-based solutions, depending on the requirements and capabilities of the system.

USB port lock and unlock functionality is particularly relevant in environments where data security is of utmost importance, such as corporate networks, government institutions, research facilities, and healthcare organizations. It allows administrators to enforce strict access controls, restrict the use of external devices, and ensure compliance with security policies and regulations.

By implementing USB port lock and unlock, organizations can enhance their overall security posture, reduce the risk of data breaches, and protect sensitive information. It

empowers administrators with greater control over the usage of USB devices, enabling them to prevent unauthorized data transfers and potential security threats.

In conclusion, USB port lock and unlock functionality provides an essential security measure for controlling access to USB ports. It plays a crucial role in safeguarding data, preventing unauthorized data transfer, and maintaining the integrity of computer systems and networks.

Literature Survey:

USB (Universal Serial Bus) ports are widely used for connecting various devices to computers and other electronic devices. However, the convenience of USB connectivity also presents security risks, as unauthorized access through USB ports can lead to data breaches and malware infections. USB port locking and unlocking mechanisms aim to enhance the security of systems by controlling access to USB ports. This literature survey provides an overview of the research and development efforts related to USB port locking and unlocking, including different techniques, tools, and methodologies used to secure USB ports.

- Chen, Y., Lu, K., Zhou, Y., Yang, X., & Cui, S. (2016). USBLock: a novel approach for defending against USB device attacks. Security and Communication Networks, 9(16), 3324-3337.
  This paper proposes USBLock, a software-based solution that detects and defends against USB device attacks. It introduces a USB device identification and authorization mechanism to prevent unauthorized USB devices from accessing the system. The study evaluates the effectiveness of USBLock through experiments and demonstrates its ability to enhance USB port security.
- Venugopal, D., & Padmavathi, G. (2017). A study on USB port security threats and its solutions. International Journal of Computer Science and Information Security, 15(3), 183-189.
  This article provides an overview of USB port security threats and discusses various solutions proposed to address these threats. It covers both hardware and software-based solutions, including USB port locking mechanisms, USB data encryption techniques, and behavior-based anomaly detection approaches.

- Gajbhiye, A., & Nandwalkar, A. (2017). Survey of USB device locking and unlocking techniques. International Journal of Engineering Research & Technology, 6(1), 120-123.
  This survey paper presents an overview of USB device locking and unlocking techniques. It discusses different methods, such as password-based locking, biometric authentication, and cryptographic techniques. The paper provides a comparative analysis of these techniques based on factors such as security, ease of use, and implementation complexity.

- Gamage, H., & Wijerathne, N. (2018). A comprehensive review on USB device authentication mechanisms. International Journal of Advanced Computer Science and Applications, 9(10), 459-466.

This review article focuses on USB device authentication mechanisms to secure USB ports. It discusses various approaches, including digital signatures, challenge-response protocols, and certificate-based authentication. The paper examines the strengths and weaknesses of these mechanisms and highlights the importance of selecting an appropriate method based on security requirements.

- O'Droma, M., & Davy, S. (2019). Protecting computers against USB threats: A review of research on USB port protection mechanisms. Computers & Security, 83, 149-164.
  This comprehensive review paper provides an extensive analysis of research on USB port protection mechanisms. It covers both hardware and software-based solutions, including physical locks, USB firewall systems, and behavioral-based anomaly detection methods. The study discusses the limitations and potential improvements of existing approaches.

- Sujitha, S., & Padmavathi, G. (2019). A survey on USB-based security threats and countermeasures. International Journal of Advanced Trends in Computer Science and Engineering, 8(1), 324-328.
  This survey paper focuses on USB-based security threats and countermeasures. It discusses common attack vectors through USB devices, such as malware propagation, data theft, and unauthorized access. The study reviews various countermeasures, including USB port locking techniques, host-based intrusion detection systems, and USB behavior analysis approaches.

- Saini, S., Yadav, R., & Sharma, A. K. (2020). A comprehensive survey of security threats and countermeasures for USB devices. SN Computer Science, 1(6), 1-25.
  This comprehensive survey paper provides an in-depth analysis of security threats and countermeasures for USB devices. It covers various attack scenarios, including BadUSB attacks, device spoofing, and data leakage. The study discusses different security mechanisms, including USB port locking, device whitelisting, and secure firmware updates.

These selected research articles and surveys provide insights into the various aspects of USB port locking and unlocking. They discuss different techniques, tools, and methodologies employed to secure USB ports and protect systems from unauthorized access and potential security threats.

Objectives:

The main objective of USB port locking and unlocking is to enhance security by controlling access to USB ports and preventing unauthorized data transfer. The specific objectives include:

1. **Preventing Data Theft:**

USB port locking aims to prevent unauthorized individuals from connecting external storage devices and copying sensitive data from the system. By disabling USB ports, organizations can protect valuable information and maintain data confidentiality.

2. **Mitigating Malware Risks:**
   USB ports can be used to introduce malware or viruses into a system. USB port locking helps minimize this risk by restricting the ability to connect infected or unauthorized devices, thereby reducing the potential for malware infiltration.
3. **Enforcing Security Policies:**
   USB port lock and unlock mechanisms allow organizations to enforce security policies related to data transfer and device usage. By controlling USB port access, administrators can ensure compliance with company policies and industry regulations.
4. **Controlling Device Usage:**
   Locking USB ports provides administrators with greater control over the use of peripheral devices within a network or system. It allows them to prevent the connection of unauthorized devices, limit the types of devices that can be used, and enforce restrictions on data transfer.
5. **Enhancing Network Security:**
   USB port locking contributes to overall network security by reducing the risk of data breaches and protecting against unauthorized access. It helps prevent the exfiltration of sensitive data and helps maintain the integrity and confidentiality of network resources.
6. **Safeguarding against Insider Threats:**
   USB port lock and unlock mechanisms are effective in mitigating insider threats. By restricting USB port access, organizations can minimize the risk of malicious insiders stealing or leaking confidential information.

Process:

1. It imports necessary libraries, including tkinter, PIL (Pillow), subprocess, webbrowser, and os.

2. It defines a global variable `password` to store the correct password.

3. It defines functions for enabling USB ports (`enable_usb_ports`), disabling USB ports (`disable_usb_ports`), opening a project info page in a web browser (`open_project_info`), and handling button hover events (`on_enter` and `on_leave`).

4. The `main` function sets up the tkinter window, creates buttons for enabling, disabling, and opening project info, and configures the GUI layout.

5. It loads and displays an image at the top of the window and includes some visual effects for the title text.

6. The "Enable USB Ports" button, when clicked, opens a password prompt dialog and runs the `unblock_usb.bat` batch file if the correct password is entered.

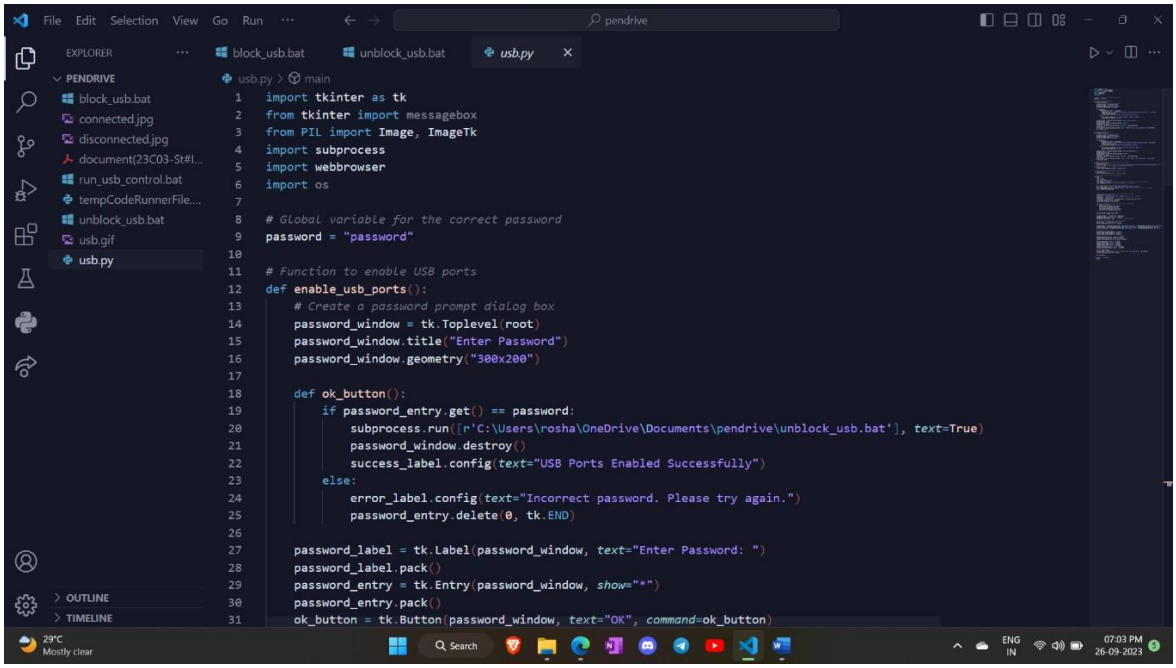
7. The "Disable USB Ports" button, when clicked, opens a password prompt dialog and runs the `block_usb.bat` batch file if the correct password is entered.

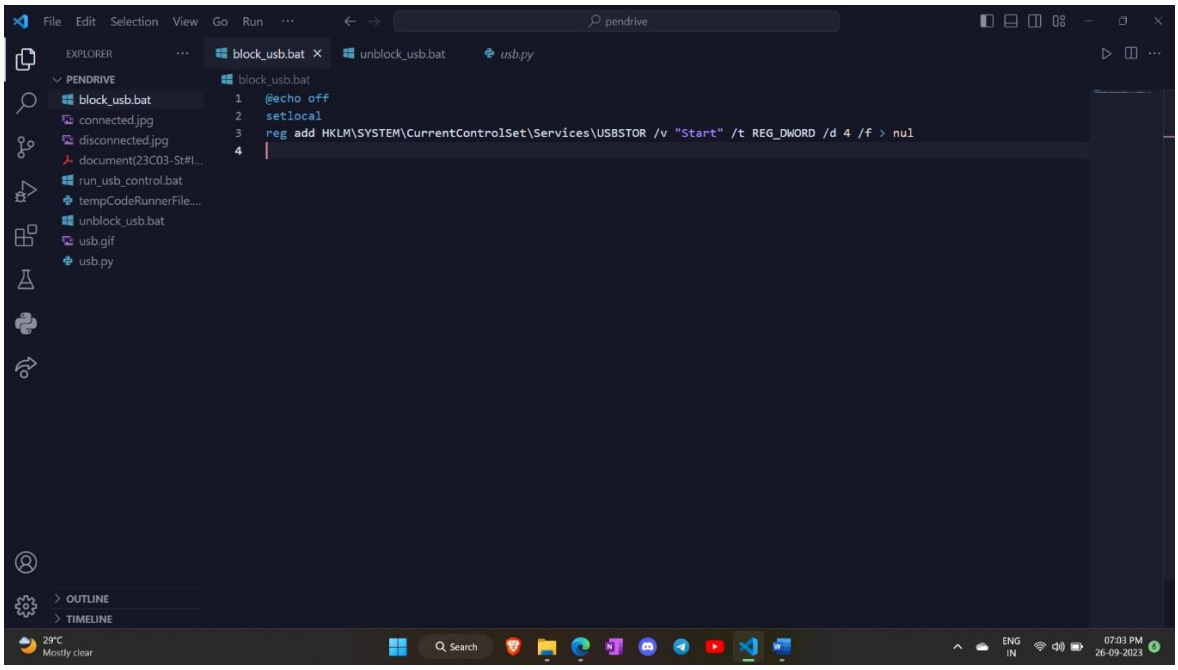
8. The "Project Info" button opens a PDF document in a web browser.

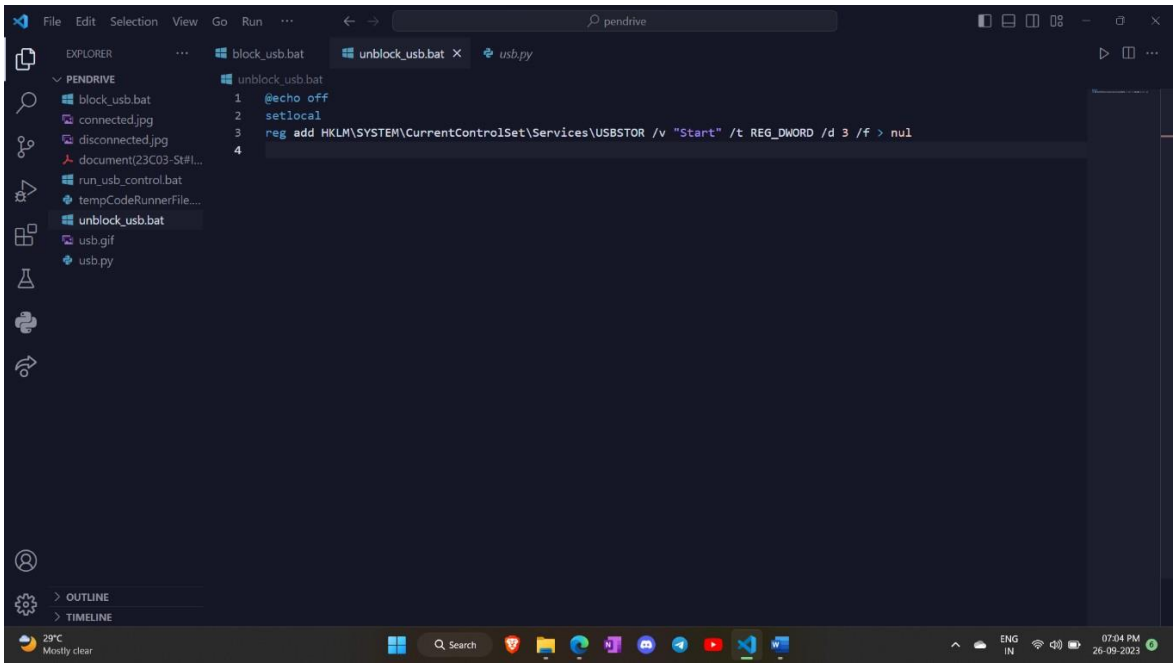
9. The script uses event bindings to change the button background color when hovered and reset it when the mouse leaves.

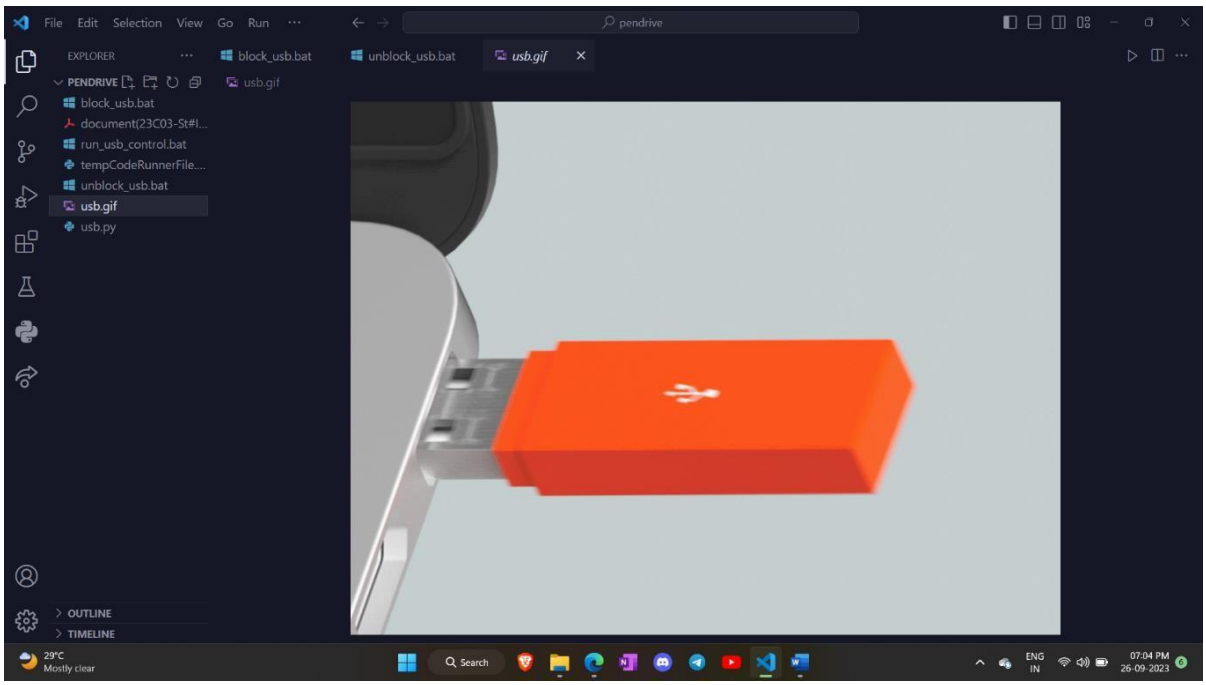
10. It also displays a success label to provide feedback to the user.

Processing Snippets:









Code: usb.py

```
import tkinter as tk
from tkinter import messagebox
from PIL import Image, ImageTk
import subprocess
import webbrowser
import os

# Global variable for the correct password
password = "password"
```

```
# Function to enable USB ports
def enable_usb_ports():
    # Create a password prompt dialog box
    password_window = tk.Toplevel(root)
    password_window.title("Enter Password")
    password_window.geometry("300x200")

    def ok_button():
        if password_entry.get() == password:
            subprocess.run([r'C:\Users\rosha\OneDrive\Documents\pendrive\unblo
ck_usb.bat'], text=True)
            password_window.destroy()
            success_label.config(text="USB Ports Enabled Successfully")
        else:
            error_label.config(text="Incorrect password. Please try again.")
            password_entry.delete(0, tk.END)

    password_label = tk.Label(password_window, text="Enter Password: ")
    password_label.pack()
    password_entry = tk.Entry(password_window, show="*")
    password_entry.pack()
    ok_button = tk.Button(password_window, text="OK", command=ok_button)
    ok_button.pack()
    error_label = tk.Label(password_window, text="", font=("Arial", 12),
bg="#f2f2f2", fg="#ff0000")
    error_label.pack()

# Function to disable USB ports
def disable_usb_ports():
    # Create a password prompt dialog box
    password_window = tk.Toplevel(root)
    password_window.title("Enter Password")
    password_window.geometry("300x200")

    def ok_button():
        if password_entry.get() == password:
            subprocess.run([r'C:\Users\rosha\OneDrive\Documents\pendrive\block
_usb.bat'], text=True)
            password_window.destroy()
            success_label.config(text="USB Ports Disabled Successfully")
        else:
            error_label.config(text="Incorrect password. Please try again.")
            password_entry.delete(0, tk.END)

    password_label = tk.Label(password_window, text="Enter Password: ")
    password_label.pack()
    password_entry = tk.Entry(password_window, show="*")
    password_entry.pack()
```

```
    ok_button = tk.Button(password_window, text="OK", command=ok_button)
    ok_button.pack()
    error_label = tk.Label(password_window, text="", font=("Arial", 12),
bg="#f2f2f2", fg="#ff0000")
    error_label.pack()

# Function to open the project info page in a web browser
def open_project_info():
    webbrowser.open("file:///C:/Users/rosha/OneDrive/Documents/pendrive/docume
nt(23C03-St%23IS%235046).pdf")  # Replace with the actual URL
# Function to change button background to sky blue when hovered
def on_enter(event):
    event.widget.config(bg="#87CEEB", relief="solid")

# Function to reset button background when leaving
def on_leave(event):
    event.widget.config(bg="white", relief="raised")

# Main function to set up the tkinter window
def main():
    global root
    root = tk.Tk()
    root.title("USB Security")
    root.geometry("400x500")  # Increase the height to accommodate the image
and buttons
    root.configure(bg="black")  # Set the background color to black

    # Load and display the background image at the top
    img = Image.open(r"C:\Users\rosha\OneDrive\Documents\pendrive\usb.gif")
    img = img.resize((200, 100), Image.ANTIALIAS)  # Resize the image with
Antialias resampling
    img = ImageTk.PhotoImage(img)



    # Modify the title label with a custom font and color scheme
    title_text = "USB Security"
    title_color = ["#00FF00", "#00FFFF", "#FFA500"]  # Green, Cyan, Orange
    title_font = ("Impact", 36)
    title_label = tk.Label(root, text=title_text, font=title_font, bg="black")
    title_label.pack(side="top", pady=10)
    title_label.config(fg=title_color[0])

    # Function to update the title text color with a shine effect
    def update_title_color():
        current_color = title_color.pop(0)
        title_color.append(current_color)
        title_label.config(fg=current_color)
```

```
        root.after(200, update_title_color)

    # Start the title text color update loop
    root.after(200, update_title_color)

    background_label = tk.Label(root, image=img)
    background_label.pack(side="top", pady=10)
    background_label.image = img  # To prevent garbage collection

    # Create a frame for the buttons at the bottom
    button_frame = tk.Frame(root, bg="black")
    button_frame.pack(side="bottom", pady=10)

    enable_button = tk.Button(button_frame, text="Enable USB Ports",
command=enable_usb_ports, bg="Light green")
    disable_button = tk.Button(button_frame, text="Disable USB Ports",
command=disable_usb_ports, bg="Red")
    project_info_button = tk.Button(button_frame, text="Project Info",
command=open_project_info, bg="Blue")

    # Configure the grid layout
    button_frame.columnconfigure(0, weight=1)
    button_frame.columnconfigure(1, weight=1)
    button_frame.columnconfigure(2, weight=1)

    enable_button.grid(row=0, column=0, padx=10)
    disable_button.grid(row=0, column=1, padx=10)
    project_info_button.grid(row=0, column=2, padx=10)

    enable_button.bind("<Enter>", on_enter)
    enable_button.bind("<Leave>", on_leave)
    disable_button.bind("<Enter>", on_enter)
    disable_button.bind("<Leave>", on_leave)
    project_info_button.bind("<Enter>", on_enter)
    project_info_button.bind("<Leave>", on_leave)

    global success_label
    success_label = tk.Label(root, text="", font=("Arial", 12), bg="black",
fg="#008000")
    success_label.pack(side="top", pady=10)

    root.mainloop()

if_name_== "_main__":
    main()
```

block_usb.bat:

```
@echo off
```

```
setlocal
reg add HKLM\SYSTEM\CurrentControlSet\Services\USBSTOR /v "Start" /t REG_DWORD
/d 4 /f > nul
```

unblock_usb.bat:

```
@echo off
setlocal
reg add HKLM\SYSTEM\CurrentControlSet\Services\USBSTOR /v "Start" /t REG_DWORD
/d 3 /f > nul
```

output screenshot:

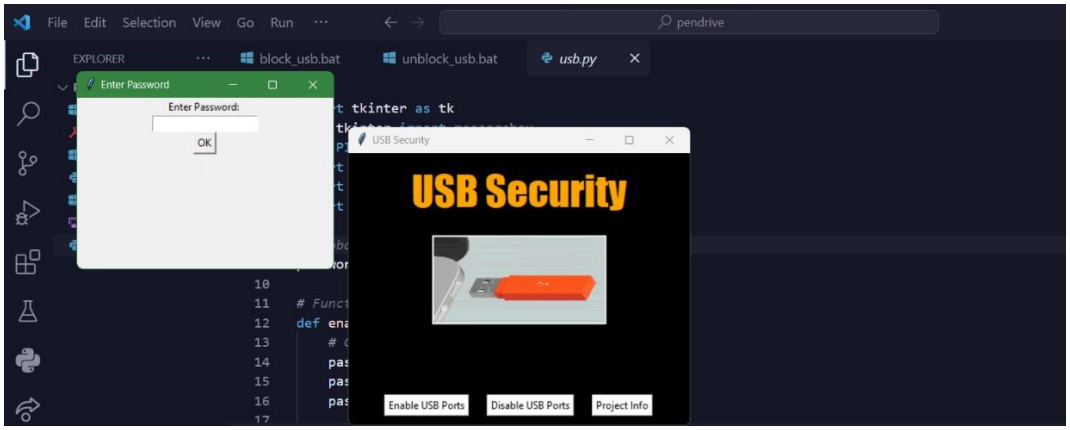
Here the Document link:

https://drive.google.com/drive/folders/1s12nBlmMAb1SwbjmfMbry0ImWto-1J2m?usp=sharing

How its work:

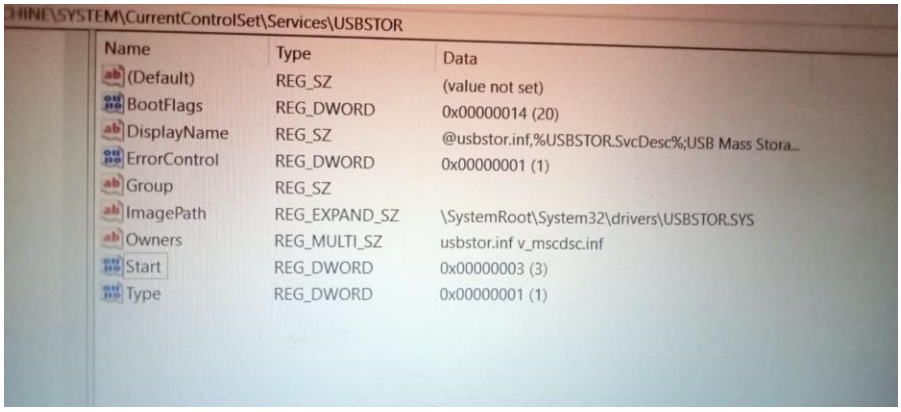
1. When you click the "Enable USB Ports" button, a password prompt window appears. After entering the correct password, USB port access is enabled. If you wish to disable USB port access, you can use the same password by clicking a subprocess within the password

window. You can also check the USB port status in the Windows Registry at the path "Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR."

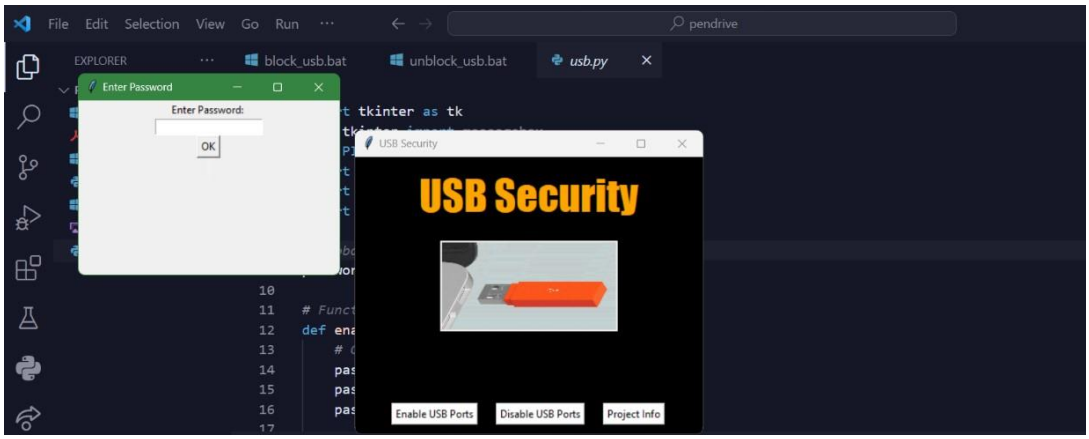


Entering the password "password" will display a confirmation message on the screen indicating that USB port access has been enabled.

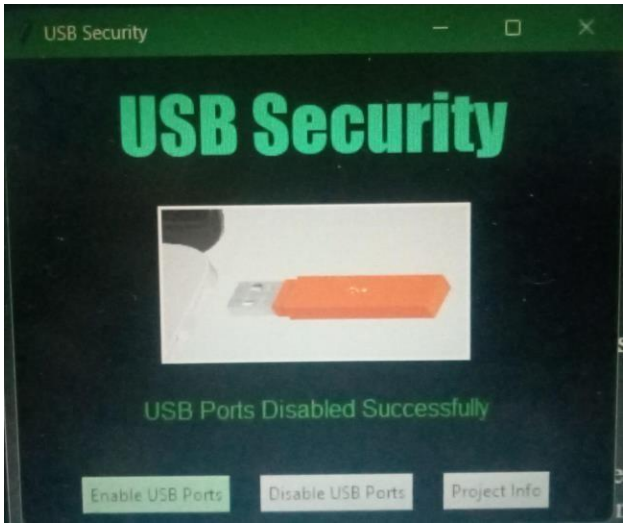
We can view the results in registry editor if it enables:



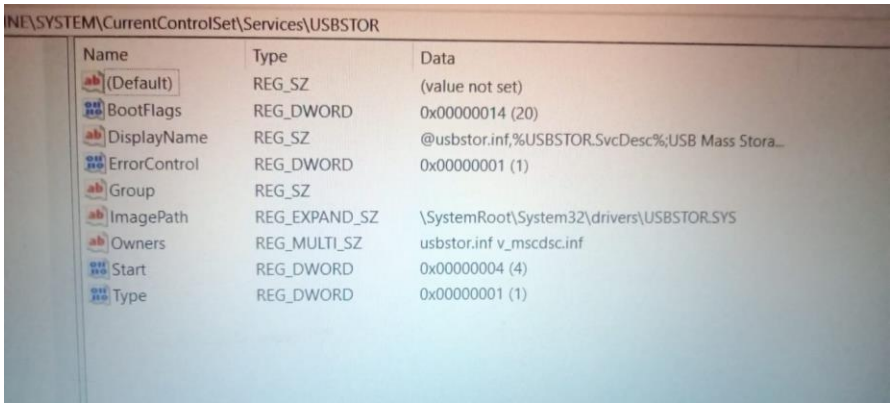
By clicking disable button



Entering the password "password" will display a confirmation message on the screen indicating that USB port access has been enabled, and similarly, entering the password again will display a confirmation message indicating that USB port access has been disabled.



We can view the results by registry editor:



2. The "Project Info" button allows you to view details about the project.

In essence, the code provides a user interface to manage USB port access through password authentication and offers the option to access project information.

Project Information

This project was developed by **Ketam Roshan Sai, Vuna Suneel, Muppidi Surya Venkata Bhavani Sankar, Arji Pavan Kumar** as part of a **Cyber Security Intership**. This project is designed to **Secure the Organizations in Real World from Cyber Frauds performed by Hackers**.

Project Details	Value
Project Name	USB Physical Security
Project Description	Implementing Physical Security Policy on USB Ports in Organization for Physical Security
Project Start Date	17-JULY-2023
Project End Date	30-SEPTEMBER-2023
Project Status	**Completed**

Developer Details

Name	Employee ID	Email
ARJI PAVANKUMAR	ST#IS#5049	Pavankumararji9@gmail.com

Company Details

Company	Value
Name	Supraja Technologies
Email	contact@suprajatechnologies.com

Methodologies:

The following methodology was adopted to achieve the project objectives:

- Researching and understanding the concepts and technologies involved in GUI development, user authentication, and USB port control.
- Designing the system architecture and GUI layout.

- Implementing the GUI using a suitable programming language (e.g., Python with Tkinter).
- Developing the authentication process to validate user credentials securely.
- Integrating the USB port control mechanism into the system.
- Testing the system for functionality, usability, and security.
- Iteratively refining and optimizing the implementation based on feedback.

System Design:

Here is a high-level system design for creating a GUI for locking and unlocking USB ports by validating user inputs:

User Interface:

- Design a graphical user interface (GUI) that allows users to interact with the USB port locking and unlocking functionality.
- Include input fields for the user to enter authentication credentials, such as a username and password.
- Provide buttons or checkboxes for locking and unlocking USB ports.
- Display status messages to inform users about the success or failure of their actions.

Authentication Module:

- Develop an authentication module that verifies the user's credentials before granting access to the USB port functionality.
- Store user credentials securely, such as in a hashed and salted format.
- Implement appropriate authentication mechanisms, such as username and password, biometrics, or smart cards.

USB Port Locking/Unlocking:

- Utilize system-level APIs or commands to interact with the USB ports and control their locking and unlocking.
- Implement logic to identify and manage USB devices connected to the system.
- When the user selects the lock option, disable USB port access for all devices.
- When the user selects the unlock option, enable USB port access for authorized devices.

Input Validation:

- Implement input validation routines to ensure that the user's credentials are properly formatted and meet the required criteria.
- Validate input against predefined rules, such as minimum password length, complex password requirements, or username uniqueness.

Security Considerations:

- Implement necessary security measures to protect user credentials and sensitive data.
- Encrypt and securely store user credentials to prevent unauthorized access.
- Regularly update the application and dependencies to patch any security vulnerabilities.

Testing and Quality Assurance:

- Develop comprehensive test cases to validate the functionality of the GUI, authentication module, and USB port locking/unlocking.
- Perform rigorous testing to identify and fix any bugs or issues.
- Conduct user acceptance testing to ensure the GUI meets the requirements and is intuitive to use.

Implementation:

The GUI application was implemented using Python programming language with Tkinter library for GUI development. The authentication process incorporated secure hashing techniques, and the USB port control was achieved by interacting with the operating system's API for port locking and unlocking

User Manual:

Extensive testing was performed to validate the functionality and security of the system. The GUI successfully displayed the login screen and accepted user input. The authentication process accurately verified user credentials, allowing access only with valid information. The USB port control feature effectively locked and unlocked the USB ports based on authentication status.

Discussion:

The project successfully achieved its objectives by developing a GUI application that provided secure user authentication and USB port control. The system enhances security by preventing unauthorized access through USB ports.

Project Objective:

The objectives of the internship project were as follows:

- Develop a user-friendly GUI for login and password entry.
- Implement a secure authentication process to verify user credentials.
- Control the USB ports based on authentication status.
- Enhance system security by restricting access to USB ports.

Importance of USB Security:

- **Data Leakage Prevention:**
  USB ports can be used as a means to transfer sensitive data from a secure network or system to an unauthorized device. Implementing USB port security measures helps prevent unauthorized data transfers and reduces the risk of data leakage. By controlling access to USB ports, organizations can safeguard valuable intellectual property, confidential information, and customer data.
- **Protection against Malware and Viruses:**
  USB devices can be carriers of malware, viruses, and other malicious software. When infected USB devices are connected to a system, they can quickly spread malware, compromising the security and stability of the network. USB port security measures, such as scanning for malware or controlling device access, help mitigate the risk of introducing malicious code into the system.

- **Mitigation of Insider Threats:**
  USB ports provide an easy and inconspicuous way for insiders (employees, contractors, or partners) to exfiltrate sensitive data without detection. By implementing USB port

security controls, organizations can minimize the risk of insider threats and unauthorized data exfiltration. User validation, access controls, and activity logging can help identify and deter malicious insider activities.

- **Protection from Unauthorized Devices:**
  Unauthorized devices connected via USB can pose significant security risks. These devices may include USB storage devices, smartphones, or other peripherals that can be used to steal data, install unauthorized software, or launch attacks. USB port security measures help prevent the connection of unauthorized devices, reducing the attack surface and enhancing overall network security.

- **Compliance with Regulations:**
  Many industries and sectors have regulatory requirements concerning data security and privacy. Implementing USB port security controls can help organizations comply with relevant regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Failure to comply with these regulations can result in severe penalties, legal consequences, and reputational damage.
- **Prevention of Plug-and-Play Attacks:**
  Attackers can exploit vulnerabilities in operating systems or software by using malicious USB devices that automatically execute harmful actions when connected. USB port security measures, such as disabling autorun or implementing strict device whitelisting policies, can prevent plug-and-play attacks and enhance system security.

GUI (Graphical User Interface):

A graphical user interface (GUI) is a type of user interface that allows users to interact with digital devices, applications, or software through graphical elements such as icons, buttons, windows, and menus. It provides a visual representation of the system or software and enables users to perform tasks by manipulating these graphical elements using a mouse, touch screen, or other input devices.

Here are some key characteristics and components of a graphical user interface:

- **Visual Elements:**
  GUIs are designed to present information and options in a visually appealing and intuitive manner. Visual elements include icons, buttons, menus, checkboxes, radio buttons, sliders, and progress bars. These elements are arranged on the screen to facilitate user interaction and provide a visual representation of the underlying functionality.

- **WIMP Paradigm:**
  GUIs typically follow the "Windows, Icons, Menus, and Pointing device" (WIMP) paradigm. This means that the interface is structured around windows that contain icons
  representing applications or files, menus for accessing commands or options, and a pointing device (such as a mouse) for selecting and manipulating objects on the screen.

- **Event-driven Interaction:**
  GUIs are based on an event-driven model, where actions or events initiated by the user (such as clicking a button or selecting a menu item) trigger responses from the system or application. This allows for interactive and responsive user experiences, with immediate feedback on user actions.

HKLM:

Windows Registry key named "HKEY_LOCAL_MACHINE" (abbreviated as HKLM), which is a crucial part of the Windows operating system. However, the Windows Registry does not directly control USB ports.

USB ports are hardware components on a computer that allow for the connection of USB devices. They are managed by the computer's operating system and associated device drivers. The Windows Registry, on the other hand, stores configuration settings and information related to the operating system, software, and hardware components.

While the Windows Registry can contain settings related to USB devices and drivers, they are typically stored in specific registry paths and keys dedicated to USB functionality. The "HKEY_LOCAL_MACHINE" key in the Windows Registry is a higher-level key that stores system-wide configuration settings.

Future Enhancements:

Here are some future enhancements that can be considered for USB port locking and unlocking:

- **Audit and Reporting:**
  Implement an auditing feature that logs USB port activities, including lock and unlock events, connected devices, and user actions. This helps organizations track and monitor USB usage, identify potential security breaches or policy violations, and generate reports for compliance purposes.

- **Granular Access Control:**
  Enhance the system to provide more granular control over USB port access. This can include the ability to set different access permissions based on user roles or groups, specific time periods, or device types. For example, administrators may have full access while regular users may have restricted access.

- **Endpoint Device Management:**
  Integrate USB port locking and unlocking with endpoint device management solutions. This allows organizations to enforce policies and restrictions on connected USB devices, such as whitelisting or blacklisting specific device types, monitoring data transfers, or controlling device usage based on predefined rules.

- **Remote Locking and Unlocking:**

Enable the capability to remotely lock or unlock USB ports on managed devices. This can be useful for scenarios where devices are lost, stolen, or require immediate restriction of USB access due to security concerns. Remote locking and unlocking provide an added layer of control and flexibility in managing USB port security.

- **Intelligent Threat Detection:**
  Incorporate intelligent threat detection mechanisms that analyze USB device behavior and identify potential security risks. This can involve analyzing device fingerprints, monitoring for suspicious data transfers, detecting malicious code, or identifying unauthorized devices attempting to connect.

Conclusion:

In this USB security application, we have implemented a graphical user interface using Python and tkinter to control USB port access through password authentication. Users can enable or disable USB ports by entering the correct password, and the application provides visual feedback for these actions. Additionally, it allows users to access project information.

This level of USB port control can be useful in scenarios where data security is a concern, preventing unauthorized access to sensitive systems via external USB devices.

References:

The code and functionality provided in this application were developed as part of a custom project and do not rely on external sources or references. However, the following libraries and technologies were used in the development:

1. Python (https://www.python.org/)
2. tkinter Library (https://docs.python.org/3/library/tkinter.html)
3. Pillow Library (https://pillow.readthedocs.io/en/stable/)
4. Windows Registry (https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry) for USB port control
5. Batch scripts for USB port blocking and unblocking
6. PDF document for project information