**CYBER SECURITY INTERNSHIP**

# Task 8: Identify and Remove Suspicious Browser Extensions

## Objective

Understand the role of VPNs in protecting privacy and secure communication.

## Tools Used

- ProtonVPN (Free Tier)  
- Windscribe (Free)  
- whatismyipaddress.com (for IP verification)

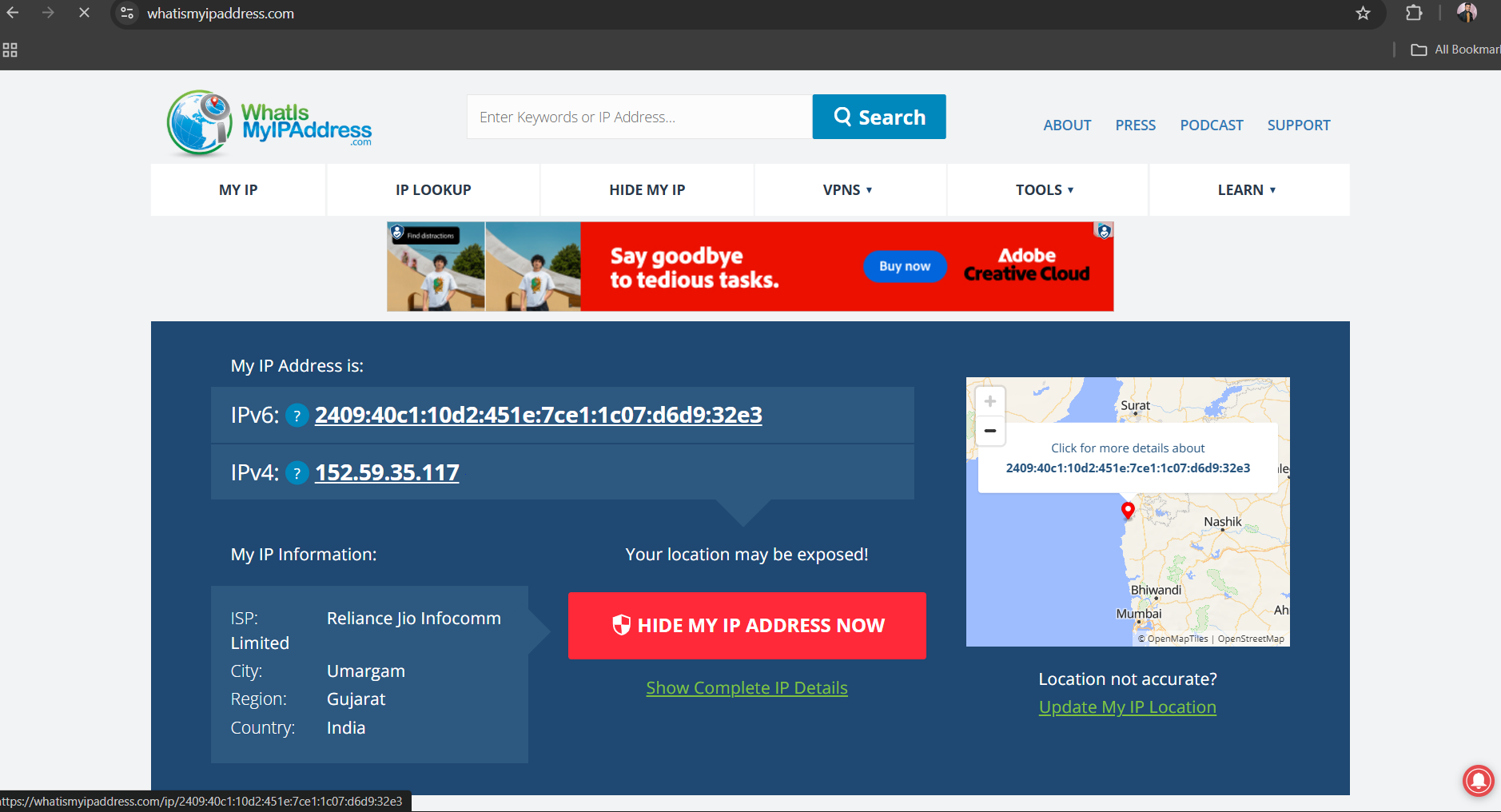
## Procedure

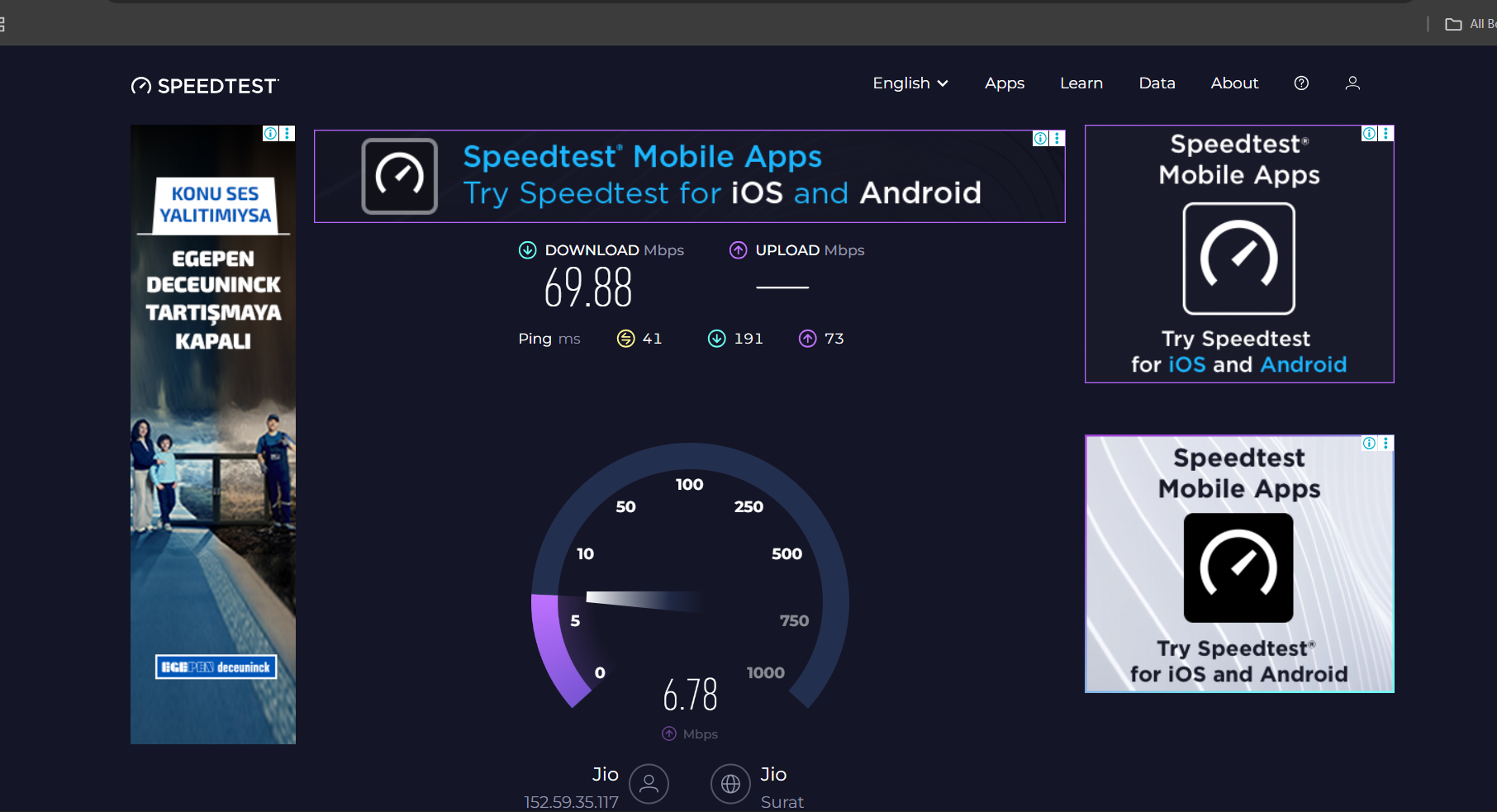
1. Downloaded and installed ProtonVPN client on Windows/Kali Linux.  
2. Signed up for a free account.  
3. Launched the VPN client and logged in.  
4. Connected to the nearest VPN server.  
5. Verified IP address change using whatismyipaddress.com.  
6. Browsed websites to confirm traffic encryption (via HTTPS).  
7. Disconnected VPN and compared browsing speed & IP.  
8. Researched VPN encryption, tunneling, and privacy features.

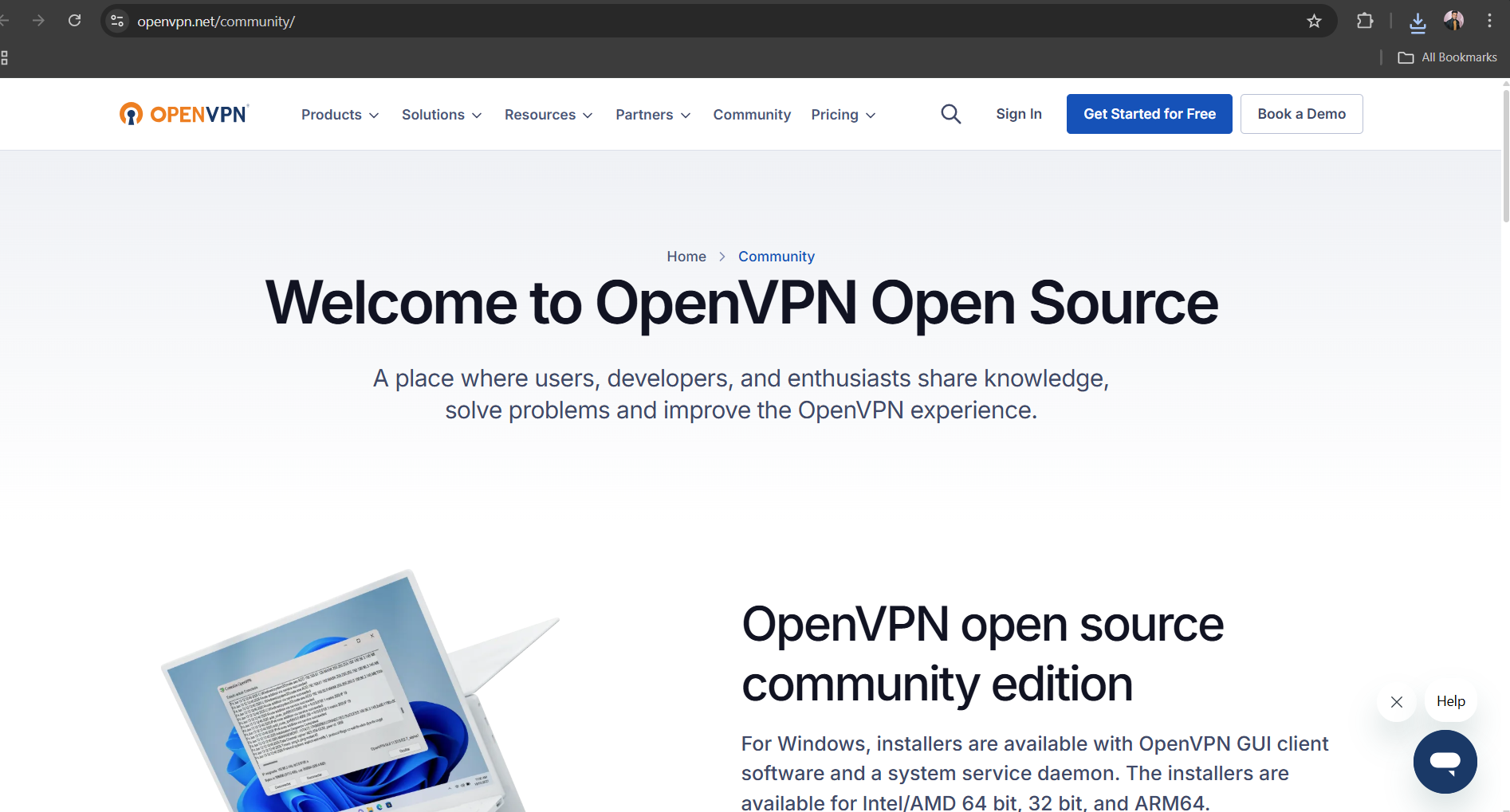
## Observations

- IP address changed successfully when connected to VPN.  
- Browsing traffic was encrypted and secure.  
- Noticed a slight decrease in browsing speed while VPN was active.  
- Without VPN, original IP and location were visible.

## Screenshots







## Summary: VPN Benefits and Limitations

Benefits:  
- Protects online privacy by masking IP address.  
- Encrypts traffic to prevent eavesdropping.  
- Helps bypass geo-restrictions.  
- Provides secure communication over public Wi-Fi.  
  
Limitations:  
- Slight reduction in internet speed.  
- Free VPNs may have limited servers and data caps.  
- VPN cannot guarantee 100% anonymity.  
- Some websites block known VPN IP ranges.

## Outcome

Hands-on experience with VPNs and better understanding of privacy tools, encryption, and tunneling protocols.