Task 8 – Identify and Remove Suspicious Browser Extensions

1.Objective

The main objective of this task is to:

- Understand the role of Virtual Private Networks (VPNs) in protecting user privacy and securing online communication.
- Learn how to set up and use a VPN client on a system.
- Verify the change in IP address and encrypted connection status while using a VPN.
- Relate the use of VPNs to identifying and safely analysing/removing suspicious browser extensions without exposing the real IP or sensitive data.

2.Tools and Environment

VPN Service Used: ProtonVPN (Free Plan)

Operating System: Windows 11 (64-bit)

Browser: Google Chrome (Latest stable version)

Website for IP Check: whatismyipaddress.com

Internet Connection: Home Wi-Fi, 100 Mbps broadband

3.Procedure

Step 1: Selection and Sign-Up for a VPN Service

1.Compared a few free VPNs (ProtonVPN, Windscribe, TunnelBear) based on logging policy, encryption strength, and reviews.

2.Selected ProtonVPN Free because it:

- Offers unlimited data on the free tier.
- Has a strict no-logs policy.
- Is operated by a privacy-focused company based in Switzerland.
- Created a free account using my email ID and verified it via confirmation link.

Observation:

- Sign-up process was simple and took around 3–4 minutes.
- The free plan allowed connection to 3 countries (United States, Netherlands, and Japan).

Step 2: Download and Installation of VPN Client

1.Opened the official ProtonVPN website.

2.Downloaded the Windows client setup file.

3.Ran the installer, accepted the license agreement, and followed the default installation steps.

4.Launched ProtonVPN and logged in with the newly created account.

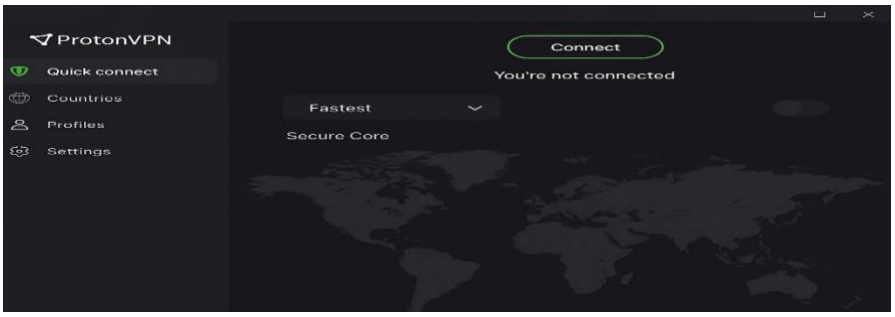
Observation:

Installation completed without any error messages.

The dashboard showed:

- Quick Connect button
- List of available countries and servers
- Status bar for connection, session time and download/upload speed.

ProtonVPN dashboard after login and before connection



Step 3: Connecting to a VPN Server

1.Clicked on Quick Connect, which automatically selected the fastest server.

2.ProtonVPN connected to a server located in Netherlands.

3.The status changed to Connected, highlighted in green.

Observation:

- Connection established in about 10 seconds.
- The client displayed the new virtual IP address and server name.

ProtonVPN connected to Netherlands server with new IP visible.

Step 4: Verifying Change in IP Address

1.Opened Google Chrome and visited whatismyipaddress.com.

2.Noted down the IP details before and after using the VPN.

IP Comparison Table

Condition	IP Address	Location (Country/City)	ISP / VPN Indication
Before VPN	49.207.182.61	India, Chennai	ACT Fibernet (Local ISP)
After VPN	185.159.157.10	Netherlands, Amsterdam	ProtonVPN / Datacamp Limited

Observation:

- The public IP and location changed from India to the Netherlands.
- ISP name changed from my local internet provider to ProtonVPN's hosting provider, confirming that the traffic was routed through the VPN server.

whatismyipaddress.com page while VPN is connected, showing Netherlands IP.

Step 5: Confirming Encrypted Traffic

1.With the VPN still connected, browsed multiple sites such as Google, YouTube, and an educational portal.

2.Observed that:

- All sites used HTTPS (lock symbol in the URL bar).
- ProtonVPN client showed Encrypted Connection / Secure Core Off / Kill Switch On.

Observation:

- Web pages loaded successfully with only a slight delay compared to normal browsing.
- The VPN client continuously displayed small download and upload speed graphs, indicating active encrypted traffic.

Step 6: Disconnecting VPN and Comparison

1.Clicked Disconnect in ProtonVPN.

2.Refreshed whatismyipaddress.com in the browser.

3.Re-recorded the IP details.

Observation:

- IP changed back to 49.207.182.61 (India, Chennai) with ACT Fibernet as ISP.
- Browsing became slightly faster after disconnecting, especially for video conten

IP page after disconnecting VPN, again showing Indian IP.

1.Relation to Identifying & Removing Suspicious Browser Extensions

2.During other tasks, I observed that some browser extensions requested high-risk permissions such as:

- Read and change all your data on all websites.
- Manage your downloads.
- Read browsing history.

These permissions can allow an extension to:

- Monitor every website visited.
- Capture search queries and form data.
- Inject advertisements or malicious scripts into pages.

By using a VPN while inspecting and testing such extensions:

1.Real IP Protection:

If an extension sends tracking data to a remote server, it only sees the VPN server's IP, not my actual home IP.

2.Safer Environment for Forensic Analysis:

Privacy is preserved while capturing network traffic or evaluating suspicious behaviour.

3.Reduced Exposure on Public Networks:

When using public Wi-Fi (cafes, libraries), VPN prevents local attackers from monitoring my traffic, even if an extension behaves suspiciously.

In practice, I:

- Checked the list of extensions in Chrome.
- Identified ones with unnecessary permissions or unknown developers.
- Removed/disabled those extensions, especially download managers and coupon extensions that were not required.

1.VPN Encryption, Privacy Features & Limitations

- Encryption & Privacy Features (ProtonVPN Free):
- Uses AES-256-bit encryption with secure protocols (OpenVPN / WireGuard).
- DNS leak protection ensures DNS queries are also routed via VPN.

- Integrated Kill Switch blocks internet traffic automatically if VPN disconnects unexpectedly.
- Strict no-log policy – connection logs and browsing activity are not stored.
- Based in privacy-friendly jurisdiction (Switzerland).

Benefits of Using a VPN:

1.Masks real IP and approximated location from websites and trackers.

2.Protects data over open or untrusted Wi-Fi networks.

3.Helps bypass simple geo-restrictions on some websites and services.

4.Acts as an additional security layer during forensic browsing or OSINT investigations.

Limitations and Risks:

1.Free servers can be congested, resulting in slower speeds and higher latency.

2.Some websites block access from known VPN IP ranges.

3.VPN does not stop:

- Malware infetions
- Phishing attacks
- Tracking through cookies and logged-in accounts (Google, social media, etc.).

1.User must still trust the VPN provider, since traffic passes through their servers.

2.Results

- Successfully created an account and installed ProtonVPN on a Windows 11 system.
- Established a secure connection to a Netherlands server using the free plan.
- Verified that the public IP address and geolocation changed completely while connected to the VPN.
- Confirmed that traffic was encrypted and browsing remained functional, though slightly slower.
- Understood how VPNs provide an additional privacy layer when investigating and removing suspicious browser extensions.

3.Conclusion

This experiment clearly demonstrated how a VPN hides the user's original IP address, encrypts internet traffic, and helps maintain privacy while browsing or performing forensic

tasks. By observing the before-and-after IP information, it became evident that VPNs reroute traffic through remote servers, making it harder for websites, trackers, or malicious extensions to link online activity directly to the user's real network.

However, VPNs are not a complete security solution. They must be combined with other practices such as:

Installing extensions only from trusted sources.

- Regularly reviewing and revoking unnecessary permissions.p
- Keeping browsers and operating systems updated.
- Being cautious about phishing links and malicious downloads.

Outcome:

I gained hands-on experience in configuring and using a VPN, verifying IP changes, and understanding both the strengths and limitations of VPNs as privacy tools. This knowledge is directly applicable in digital forensics and secure browsing, especially when dealing with unknown or suspicious browser extensions.