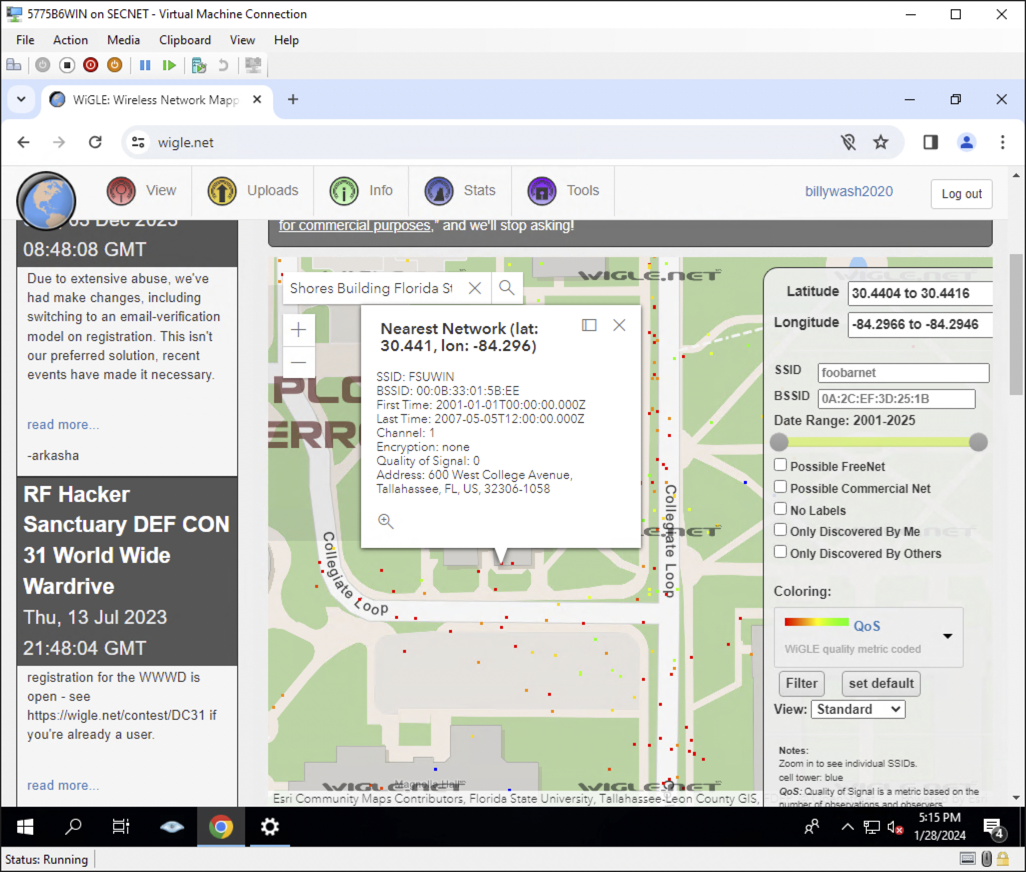
A screenshot of a computer

Description automatically generated

1. FSU on wigle.net



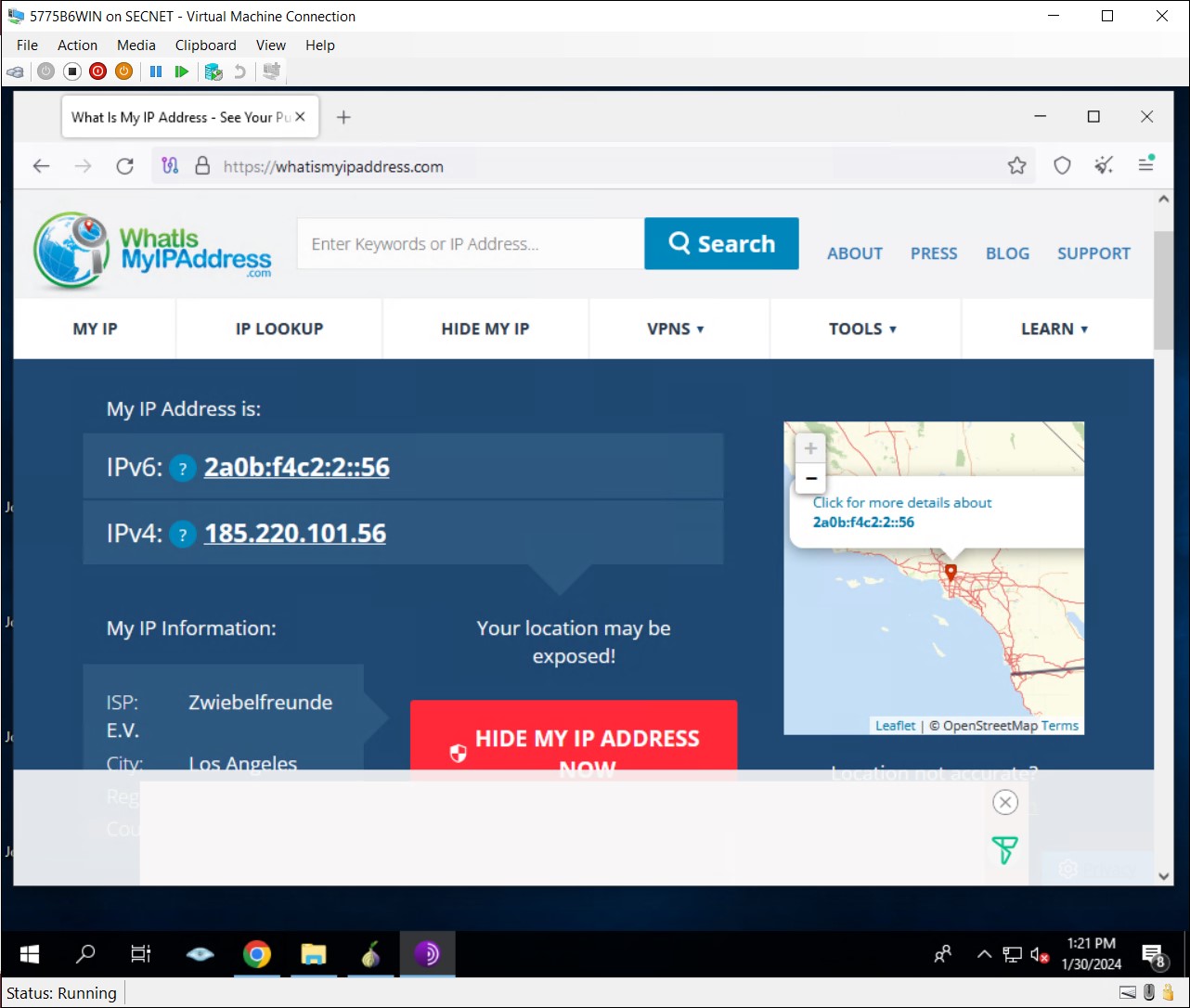
1. SSIDs over Shore Building

A screenshot of a computer

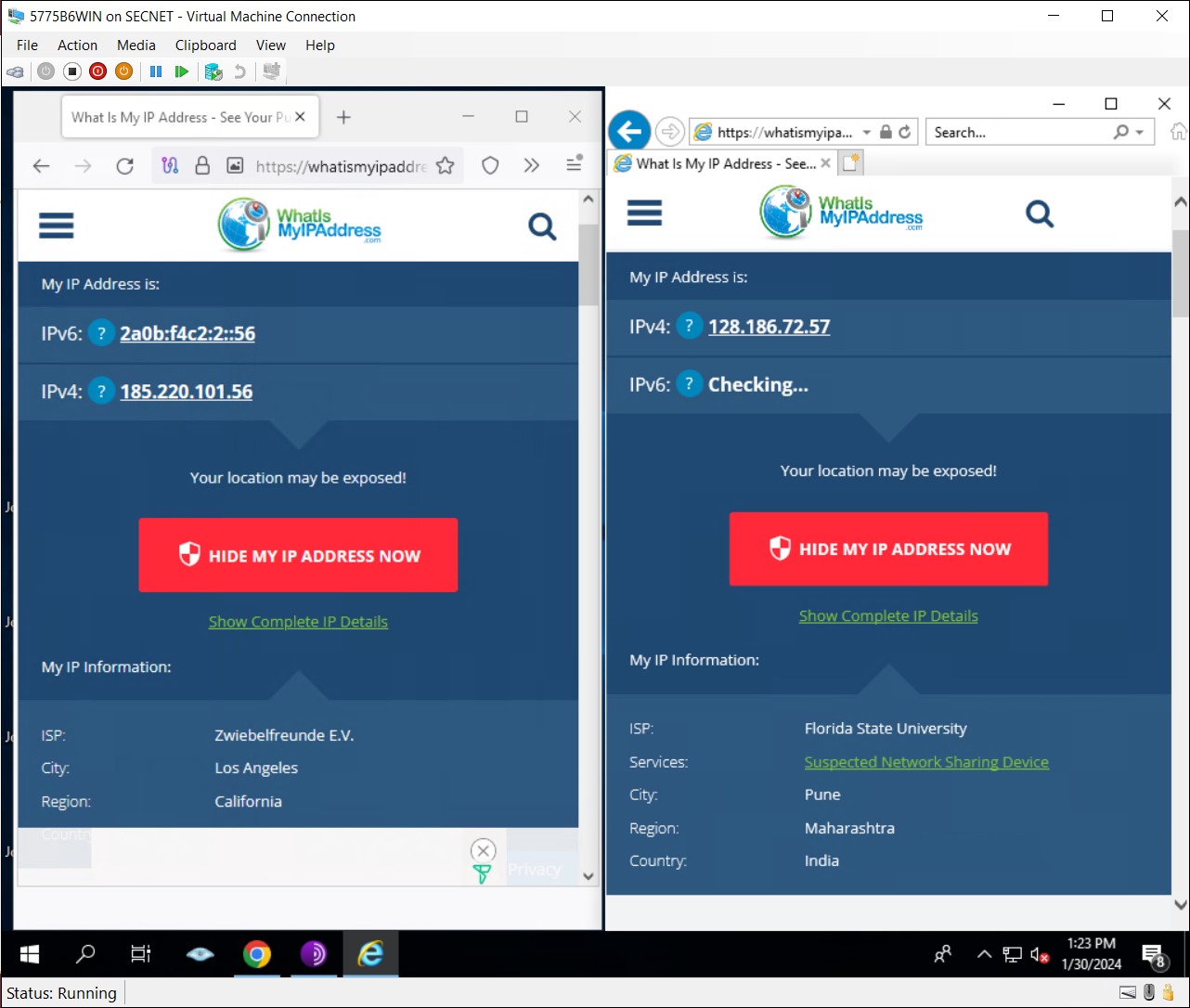
Description automatically generated

1. A screenshot of a computer

   Description automatically generatedSattelite view on wigle.net of London
2. My IP Address



1. My IP address in Tor Browser



1. My IP address in regular and Tor Browser side by side
2. What are channels? Would one be better than another?

Channels are frequency bands in Wi-Fi, dividing the spectrum to prevent interference. The optimal channel depends on factors like network traffic and interference. Choosing the right channel is crucial for optimal network performance.

1. Why is WEP considered cryptographically weak?

WEP has a 40/104-bit key size, a guessable initialization vector (IV), and vulnerabilities in its encryption algorithm. These weaknesses make it susceptible to easy exploitation and unauthorized access. WPA or WPA2 is recommended for stronger security.

1. What is the difference between WPA and WPA2?

WPA (Wi-Fi Protected Access) uses Temporal Key Integrity Protocol (TKIP) encryption, offering better security than WEP but considered less secure than WPA2.

WPA2 (Wi-Fi Protected Access 2) utilizes Advanced Encryption Standard (AES) encryption, providing superior security. It's the recommended standard for Wi-Fi networks.

1. Why do some networks run at 11 Mbps and others at 54 Mbps?

Wi-Fi speeds differ based on standards. 802.11b operates at 11 Mbps, while 802.11g and 802.11n can achieve speeds up to 54 Mbps or higher. Technological advancements contribute to these speed variations.

1. Why would someone want to use a Tor network?

The Tor network enables anonymous communication by routing internet traffic through a series of volunteer-operated servers. This helps mask the user's identity and online activities.

1. What do relay servers do in a Tor network?

Relay servers in the Tor network act as intermediaries, forwarding encrypted traffic between users and destinations. There are entry, middle, and exit relays, contributing to layered encryption for enhanced anonymity.

1. How do Tor networks provide anonymity?

Tor provides anonymity through onion routing. Traffic is encrypted in layers, and each relay decrypts only one layer, making it challenging to trace both the source and destination. The decentralized, volunteer-operated nature enhances anonymity.

1. Why is it still important to use an HTTPS connection if you are using a Tor network?

While Tor encrypts traffic within the network, it doesn't encrypt data once it leaves. HTTPS ensures end-to-end encryption between the user and the destination website, safeguarding against potential eavesdropping and tampering of data after it exits the Tor network. Always use HTTPS for comprehensive security with Tor.