CHAPTER I

INTRODUCTION

A phone hotspot can be a serious collaboration tool for a group of people attempting to work together. It works just like a dedicated mobile hotspot, but because it's inside your phone, there's nothing extra to charge, and carry. When the phone is connected to the mobile data network, it can convert the data stream into a Wi-Fi signal for other devices to share. The phone can still view web sites on its screen, make calls and respond to texts while it's hosting the connection.

At its essence, a hotspot is a blend of software, hardware and network data services that combine to transform a phone into the equivalent of a broadband modem and router. In other words, it can distribute a web connection to nearby systems via Wi-Fi.

Tethering, or phone-as-modem (PAM), is the sharing of a mobile device's Internet connection with other connected computers. Connection of a mobile device with other devices can be done over wireless LAN (Wi-Fi), over Bluetooth or by physical connection using a cable, for example through USB. If tethering is done over WLAN, the feature may be branded as a personal or mobile hotspot, which allows the device to serve as a portable router. Mobile hotspots may be protected by a PIN or password. The Internet-connected mobile device can act as a portable wireless access point and router for devices connected to it.

Many mobile devices are equipped with software to offer tethered Internet access. Windows Mobile 6.5, Windows Phone 7, Android (starting from version 2.2), and iOS 3.0 (or later) offer tethering over a Bluetooth PAN or a USB connection. Tethering over Wi-Fi, also known as Personal Hotspot, is available on iOS starting with iOS 4.2.5 (or later) on iPhone 4, 4S (2010), 5, iPad (3rd generation), certain Windows Mobile 6.5 devices like the HTC HD2, Windows Phone 7, 8 and 8.1 devices (varies by manufacturer and model), and certain Android phones (varies widely depending on carrier, manufacturer, and software version).

On some mobile network operators, this feature is contractually unavailable by default, and may only be activated by paying to add a tethering package to a data plan or choosing a data plan that includes tethering. This is done primarily because with a computer sharing the network connection, there may well be a substantial increase in the customer's mobile data use, for which the network may not have budgeted in their network design and pricing structures.[6]

Some network-provided devices have carrier-specific software that may deny the inbuilt tethering ability normally available on the device, or only enable it if the subscriber pays an additional fee. Some operators have asked Google or any mobile device producer using Android to completely remove tethering support from the operating system on certain devices. Handsets purchased SIM-free, without a network provider subsidy, are often unhindered with regards to tethering.

In order to improve the mobile hotspot, we can:

- Place the router in a strategic spot, an area where it can best broadcast signals. The goal here is to cover as many devices as possible. Wireless signals reach only up to 100 feet indoors and 300 feet outdoors. The signals can pass through floors, walls and ceilings, but fewer obstructions will result in better transmission.
- Reduce the Wi-Fi range for longer battery life. If your settings allow, tweak your mobile wireless network for low-power, shorter Wi-Fi. Users must move closer to the hotspot for better Internet connection.
- Watch out for background apps**.** Laptops, tablets, and smart phones may be running applications in the background that are using up Internet bandwidth. The most common examples of these apps are location-based services, social media and email. Minimize the amount of data you use by disabling background apps you don’t need.

- Avoid multimedia usage. Loading an email or text on a webpage with your mobile device will consume minimal amounts of data. Streaming videos or music will require more bandwidth, using up more data. Try to avoid using multimedia so your battery and data plan lasts longer.[13]

A virtual private network (VPN) extends a private network across a public network, and enables users to send and obtain information across pooled or public networks as if their computing maneuvers were directly associated to the cloistered system. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network. The technology for implementing VPNs has been in existence for some time. Their origins can be found in the Virtual Circuit. Virtual circuits are easy to implement in highly connected networks as well as being cost effective. The major benefit of VPNs, from the consumer's point of view, is that they are considerably cost effective. The alternative to using VPN technology is the high-speed leased line. These lines are expensive, difficult to administrate, and difficult to maintain.

VPNs can be characterized as host-to-network or remote access by connecting a single computer to a network or as site-to-site for connecting two networks. In a corporate setting, remote-access VPNs allow employees to access the company's intranet from outside the office. Site-to-site VPNs allow collaborators in geographically disparate offices to share the same virtual network. A VPN can also be used to interconnect two similar networks over a dissimilar intermediate network, such as two IPv6 networks connected over an IPv4 network.[17]

Cool-Tether is an architecture that provides energy-efficient, affordable connectivity by leveraging one or more WiFi equipped and Internet-enabled smartphones. The key idea is to harness the available smartphones to build an on-the-fly WiFi hotspot that is both energy-efficient and easy to use. Using Cool-Tether, a user’s laptop, at home or on the move, can obtain Internet connectivity via the user’s smartphone, thereby avoiding the need for a separate wide-area (WAN) connection and the attendant subscription costs. Smartphones are a natural fit for serving as a communication gateway for other devices, given that they are typically equipped with both local-area radios (e.g., Bluetooth or WiFi) and wide-area radios (e.g., GPRS, EDGE, 3G).

A common solution adopted today is to use the ‘tethered mode’ operation of mobile phones, allowing a dedicated phone to be used as a modem to provide connectivity to another device. This typically involves making a wired connection (e.g., using USB) or to use WiFi in ad hoc mode or Bluetooth to connect the client to the smartphone gateway.

However, neither of these approaches are satisfactory. The WiFi ad hoc mode solution is not designed to be energy efficient and ends up draining the battery of the smartphone very quickly. The Bluetooth solution incurs a high latency for discovery and connection setup and is less energy efficient than WiFi for bursty data traffic such as Web browsing. The USB cable solution is not convenient and does not support the use of more than one gateway device or smartphone, whereas, in many situations, more than one smartphone is available for use as a gateway.

To address the two key challenges of energy efficiency and multiple gateway support, Cool-Tether employs several novel techniques that focus on optimizing the energy drain of the WAN and WiFi radios on the smartphones. Cool-Tether employs a proxy in the cloud that first gathers all necessary data before commencing a bursty transmission over the WAN link. The key insight is that for maximum energy efficiency, the radio should be used for as long a burst as can be sustained at the full data rate.

In the case of WiFi, Cool-Tether adopts a novel reverse infrastructure mode of operation to accomplish tethering. In contrast to the typical WiFi infrastructure setting, where the gateway device serves as the access point (AP), the gateway device (smartphone) plays the role of a WiFi client and associates with the laptop client that acts as a WiFi Access Point in order to establish the tethering connection. Compared to either WiFi’s infrastructure mode or ad hoc mode, the reverse-infrastructure mode used by Cool-Tether offers greater energy efficiency since it allows the gateways (i.e., smartphones) to put their WiFi interfaces to sleep more effectively when not in use.

SECURITY THREATS

- Evil Twins – Rogue Wi-Fi Hotspots: One of the most common ways of obtaining sensitive information is for a cybercriminal to set up an evil twin hotspot. This is a fake Wi-Fi access point that masquerades as the legitimate access point, such as one offered by a coffee shop or hotel. An SSID could be set up like the name of the establishment. Any information disclosed while connected to that hotspot can be intercepted.
- Packet Sniffers: Using a packet sniffer, a hacker can identify, intercept, and monitor web traffic over unsecured Wi-Fi networks and capture personal information such as login credentials to bank accounts and corporate email accounts. If credentials are obtained, a hacker can gain full control of an account.
- File-Sharing: Many people have file-sharing enabled on their devices. This feature is useful at home and in the workplace, but it can easily be abused by hackers. It gives them an easy way to connect to a device that is connected to a Wi-Fi hotspot. A hacker can abuse this feature to drop malware on a device when it connects to a hotspot.
- Shoulder Surfing: Not all threats are hi-tec. One of the simplest methods of obtaining sensitive information is to observe someone's online activities by looking over their shoulder. Information such as passwords may be masked so the information is not visible on a screen, but cybercriminals can look at keyboards and work out the passwords when they are typed.
- Malware and Ransomware: When connecting to a home or work network, some form of anti-malware control is likely to have been installed, but those protections are often lacking on public Wi-Fi hotspots. Without the protection of AV software and a web filter, malware can be silently downloaded.

  We can reduce risk by providing comprehensive training to all to make sure that they are aware of the risks from public Wi-Fi hotspots and to make sure that they should only connect to public Wi-Fi networks if they use a VPN.

CHAPTER II

LITERATURE REVIEW

Anand Balachandran et.al (2003) conducted research on Wireless Hotspots: Current Challenges and Future Directions. They have tried to address the challenges using example scenario along with technological challenges and alternative approaches to connectivity highlighted several technical and deployment-related challenges that need to be addressed before such connectivity can be provided ubiquitously through Wi-Fi hotspots. These challenges include authentication, security, coverage, network management, billing, and interoperability.

Carlos J. Costa et.al (2004) conducted an exploratory study on the Business models for Hotspot. They analyze the literature in order to clarify the concept of business model and to identify hotspots business models. Based in those models an in a set of interviews they produced a hotspot business infrastructure model. This model was used to analyze hot spot "industry", what allowed the identification of several conclusions related to actors' modus operandi. They analyzed the information of the main public hotspot in order to improve this model. The next step consists of identifying the business models related to hotspot.

Adel Ismail Al-Alawi (2006) conducted research on WiFi Technology: Future Market Challenges and Opportunities. The implementation of WiFi with respect to future market opportunities in the Kingdom of Bahrain was discussed in this study. Finally, an analysis of various demographics was outlined with particular concentration on the acceptance of WiFi by society in the Kingdom of Bahrain. Some concerns along with recommendations, which need to be taken into account when using WiFi are also outlined.

Vishnu Navda et.al (2009) conducted research on Cool-Tether: Energy Efficient On-the-fly WiFi Hot-spots using Mobile Phones. They considered the problem of providing ubiquitous yet affordable Internet connectivity to devices at home, at work, and on the move. In this context, they took advantage of two significant technology trends: the commditization of WiFi WLAN technology and the rapid growth of cellular data services. They proposed an architecture called Cool-Tether that harnesses the cellular radio links of one or more mobile smartphones in the vicinity, builds a WiFi hotspot on-the fly, and provides energy-efficient, affordable connectivity.

Huaqing MAO et.al (2012) conducted a comparative research on SSL VPN and IPSec VPN. In this paper, two kinds of VPN : IPSec and SSL VPN are studied in detail, and the scope of application, security, scalability and other aspects are analyzed and compared, advantages and inadequacy are summarized, finally, VPN selection reference standard is proposed. The respective advantages and disadvantages of two VPN are concluded, finally, how to select VPN technologies is given.

Steffen Schulz et.al (2012) conducted research on Tetherway: A Framework for Tethering Camouflage. They have tried to mention the problems related to the model and architecture, to analyze the network characteristics available to network providers to detect tethering customers. We present and categorize possible detection mechanisms and derive cost factors based on how well the approach scales with large customer bases. For those characteristics that appear most reasonable and practical to deploy by large providers, we present elimination or obfuscation mechanisms and substantiate our design with a prototype Android App. They have tried to present the first general analysis and classification of tethering detection techniques.

LUO Zhiyong et.al (2013) conducted research on VPN Secure Networking Model. The aim is to design and implement a secure and reliable VPN networking model on the basis of studying of VPN network. This model uses a digital certificate authentication and an AES encryption to transfer data, and has the function of anti-replay attack. Tests show that the model supports a variety of network protocols and go through the network equipment, which is suitable for the needs of network development. This paper introduces the VPN (Virtual Private Network) technology and designs and implements a secure VPN network, then the VPN system performance tests on the Windows platform.

Tripti Sharma et.al (2015) conducted research on Security in Virtual private network application scope, operation complexity, security and scalability for IPSec VPN and SSL VPN are compared and analyzed, respective advantages and disadvantages of two VPN are concluded, finally, how to select VPN technologies is given. The methods and technology used are to minimize usage of CPU and memory as well as Comparison between two different platform of VPN based on hardware. The paper also mentions regarding the Five phases for development of test bed process: Planning, Design, Implementation, Testing, Compare, and Compile.

Kuwar Kuldeep et.al (2016) conducted research on A New Approach For The Security of VPN. An implementation scenario of a very robust, complex, advance and secure method of encryption algorithm i.e. multi-phase encryption algorithm is used here. Due to its complexity and number of operations it will be only used for payload encryption in a VPN packet. Modern emerging trends and technologies such as social media, file sharing apps, utility apps tracks user's data which is being recorder for enhancing app experience. These trends bring private and confidential data of the user into the public Internet which is vulnerable to theft or abuse by any attacker or intruder. Thus a more complex and secure communication medium is required to make positive use of the modern digital services developed for mankind. The advantages of the multi-phase encryption algorithm is that it addresses the problem of data theft, tampering or misuse if VPN connection is hijacked or abused. Therefore if the service is compromised, anyhow data will always remain safe and secure. Additionally, the disadvantage of this proposed method is it will require more computing resources in both ends of the communicating party.

K. Karuna Jyothi et.al (2018) conducted a Study on Virtual Private Network (VPN), VPN's Protocols and Security. They categorized all the different types of VPNs and noted that their flexibility allows the customer to choose which facilities are desired. VPNs can offer a variety of encryption, authentication, and integrity algorithms. The company can formulate a security profile for their offices and choose the VPN solution best suited to their needs. They examined in detail the various protocols used in VPNs and noted that, due to VPN technology being new, no one standard has yet been adopted by a clear majority. VPNs are still in their infancy and the full potential for VPNs is yet to be exploited. VPNs are promising for the future for secure communication via the Internet. It is expected that the VPN industry will be very big market in the following years. It is important that the chosen standards suit the customer's needs and that their flexibility is maintained. VPNs are a flexible, low-cost, highly secure communication tool. The development of this new technology over the next few years could well define the standard for secure communication across the Internet.

CHAPTER III

AIM AND OBJECTIVES

AIM

The main aim is to try and achieve device information security by VPN tethering.

OBJECTIVE

- To determine the extent of security level provided by the Virtual Private Network application.
- To check whether the shared device is having any change in the ip address to the actual device.

CHAPTER IV

MATERIALS AND METHODOLOGY

MATERIALS REQUIRED

Operating system: Windows, Android, iOS

VPN application used: GO VPN, VPN Super Unlimited Proxy

METHODOLOGY

I tried to see whether the device information can be hidden while sharing hotspot. So in order to work with the device information hiding, the VPN was tethered via hotspot to see if there are any changes happening. The same method can be followed in other operating systems as well.

1. **ENABLING Wi-Fi HOTSPOT:** The method may vary by phone manufacturer and Android version. Open the Settings app: (shown in Figure 1.1)

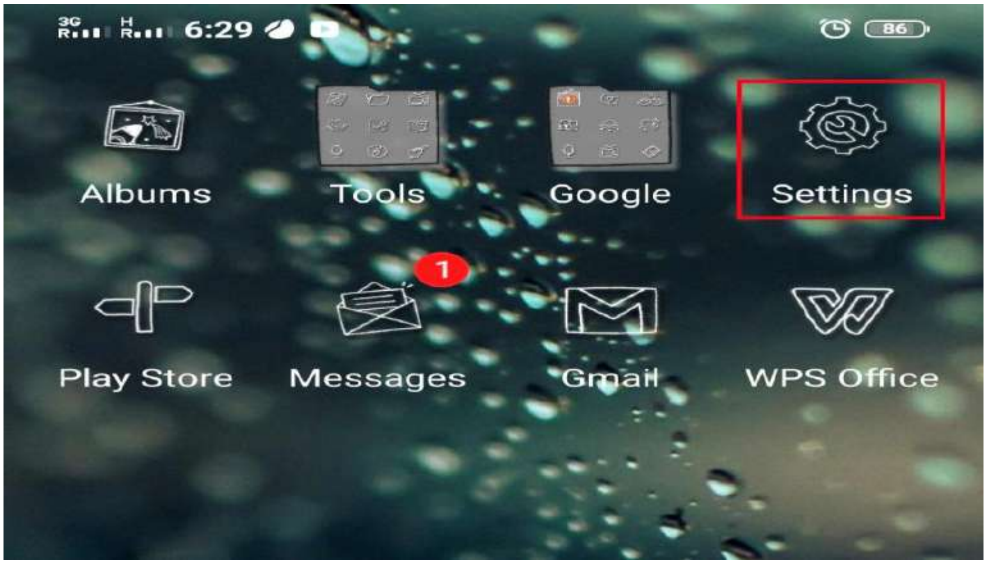
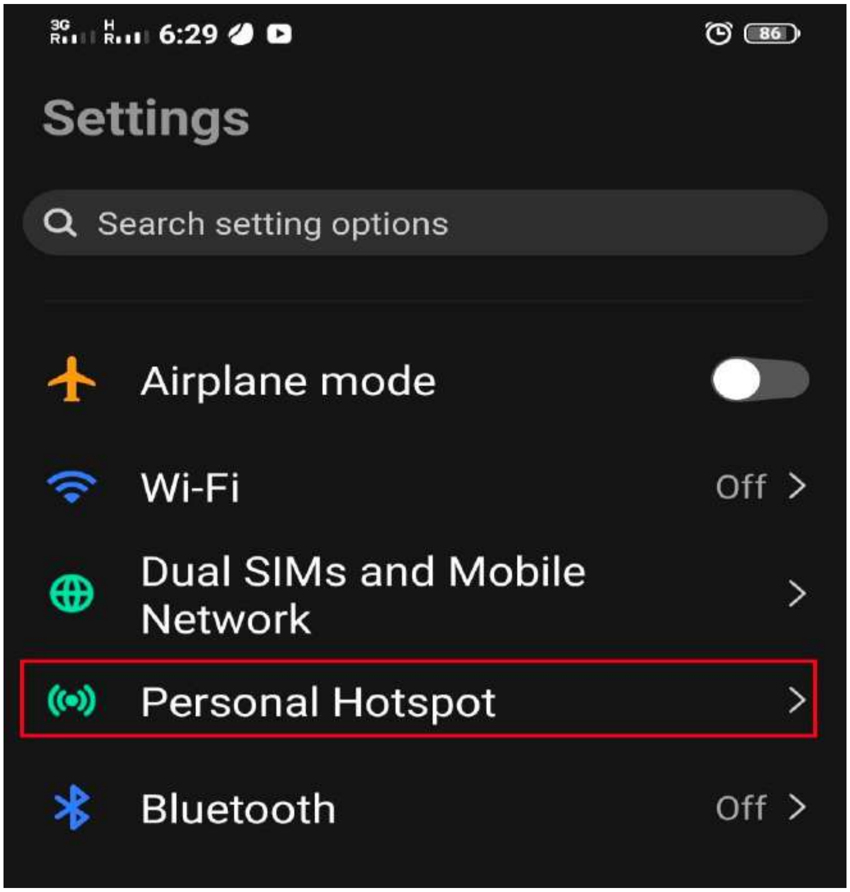


Figure 1.1: Settings app

1. Select Personal Hotspot;(shown in Figure 1.2)



Settings

Search setting options

Airplane mode

Wi-Fi Off

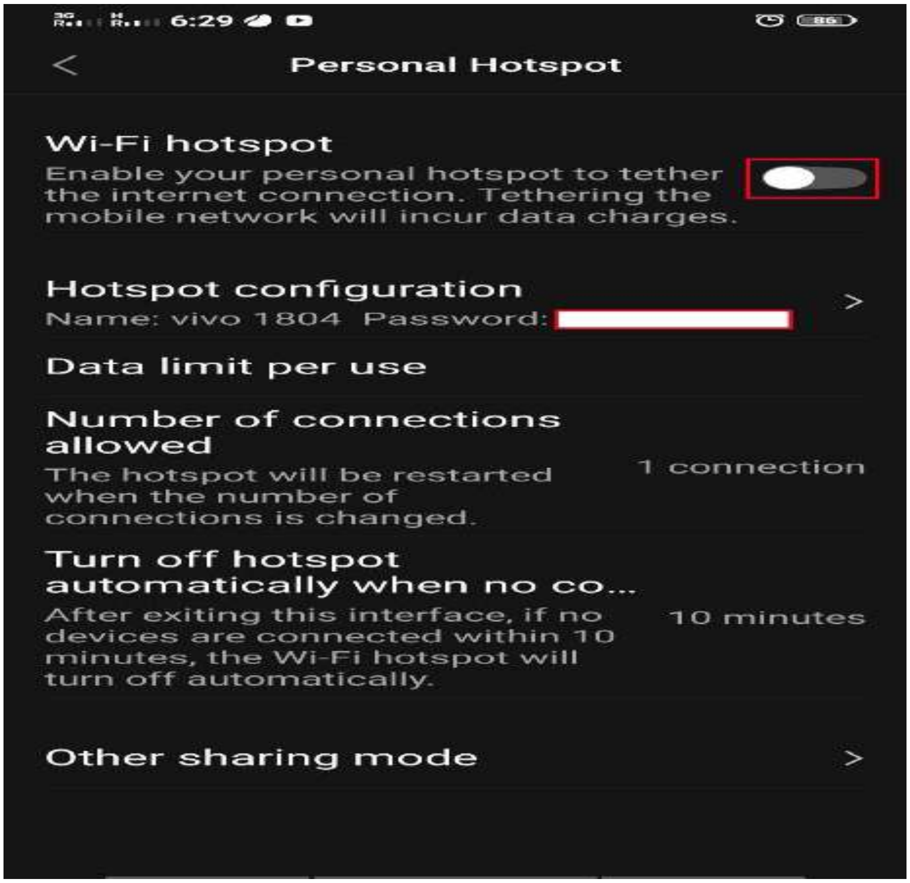
Dual SIMs and Mobile Network

Personal Hotspot

Bluetooth Off

Figure 1.2: Personal Hotspot

2. Tap on Wi-Fi hotspot; :(shown in Figure 1.3)



6:29

Personal Hotspot

Wi-Fi hotspot
Enable your personal hotspot to tether the internet connection. Tethering the mobile network will incur data charges.

Hotspot configuration
Name: vivo 1804 Password: [redacted]

Data limit per use

Number of connections allowed — 1 connection
The hotspot will be restarted when the number of connections is changed.

Turn off hotspot automatically when no co... — 10 minutes
After exiting this interface, if no devices are connected within 10 minutes, the Wi-Fi hotspot will turn off automatically.

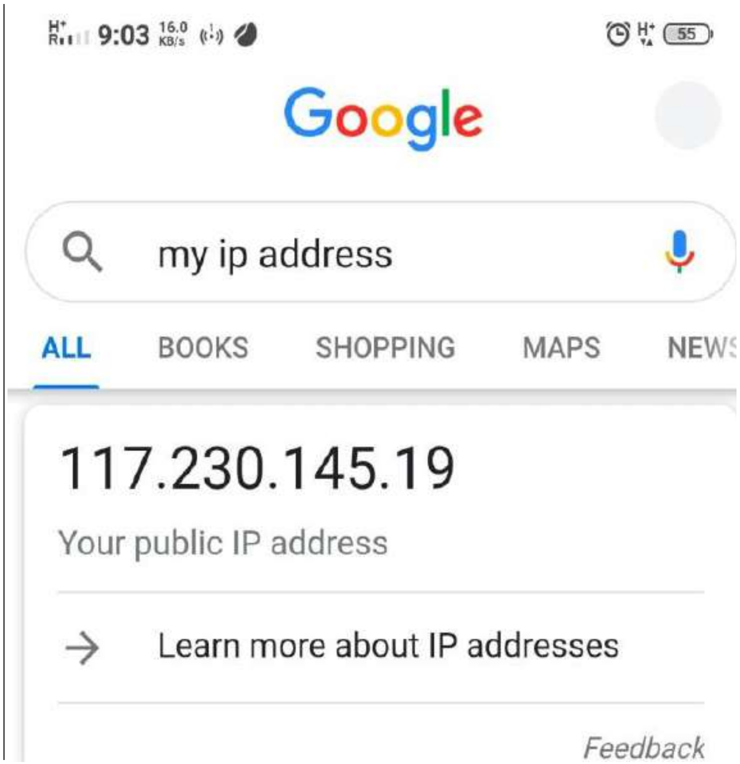
Other sharing mode

Figure 1.3: Turning on mobile hotspot

3. This page has options for turning the hotspot feature on and off. Additionally, you can change the network name, security type, password, and more;
4. Follow instructions to customize the hotspot feature to your liking.

Checking The IP Address

IP in mobile phone: (shown in Figure 1.4)



my ip address

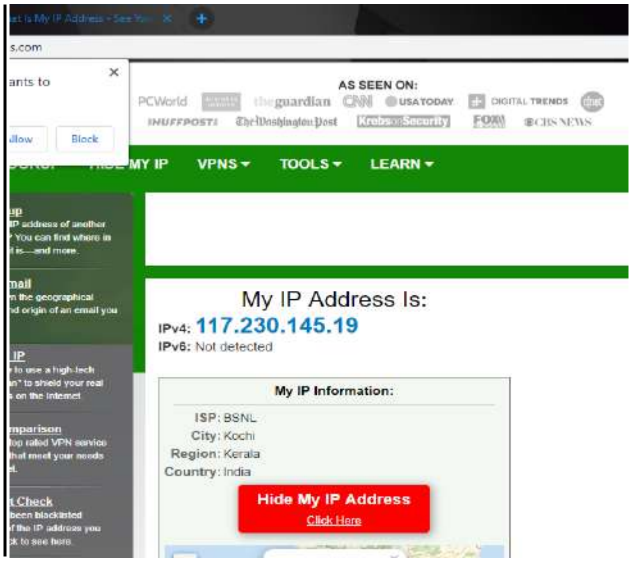
117.230.145.19

Your public IP address

Learn more about IP addresses

Figure 1.4: IP shown in the mobile phone

IP in hotspot shared laptop device: (shown in Figure 1.5)



My IP Address Is:

IPv4: 117.230.145.19

IPv6: Not detected

My IP Information:

ISP: BSNL
City: Kochi
Region: Kerala
Country: India

Figure 1.5: IP shown in laptop

The evaluations were done on the basis of difference that is seen when connected to a hotspot in two scenarios: without using a VPN and when the VPN is being used for hotspot tethering.

i. ENABLING VPN

Step 1: Choose the application from menu and open it. :(shown in Figure 1.6)

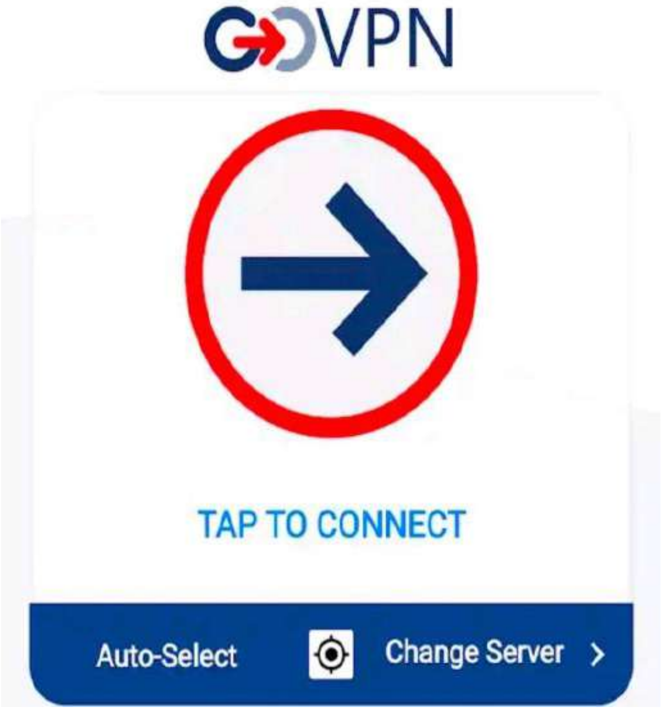
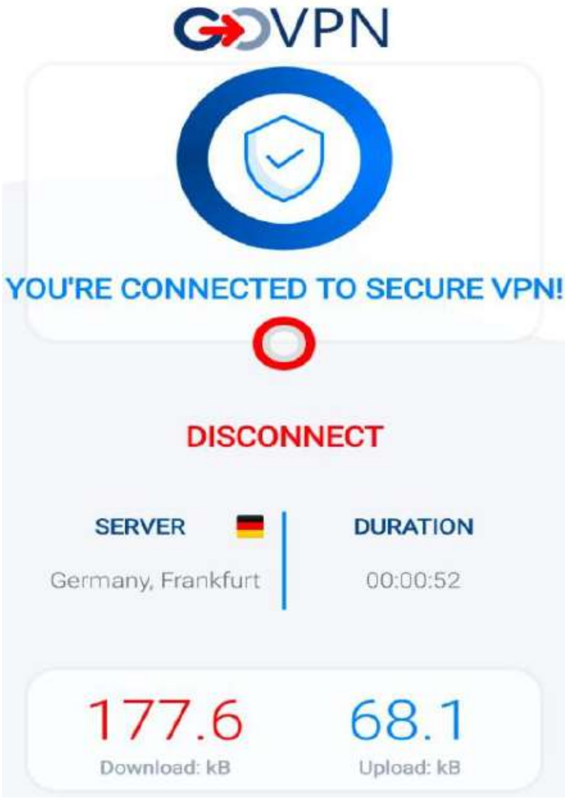


Figure 1.6: Connection to VPN

Step 2: Tap on the arrow mark to connect to the VPN and the auto-select option can be changed to choose the country according to custom desire. (shown in Figure 1.7)



SERVER Germany, Frankfurt

DURATION 00:00:52

177.6 Download: kB

68.1 Upload: kB

Figure 1.7: VPN Connection established

IN iOS

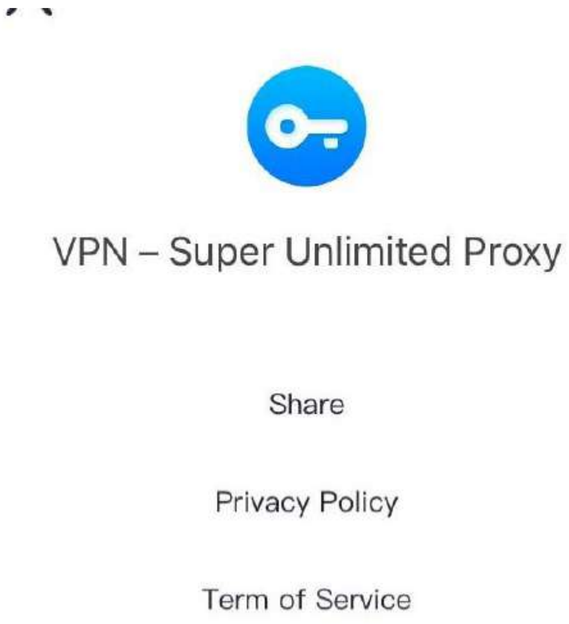
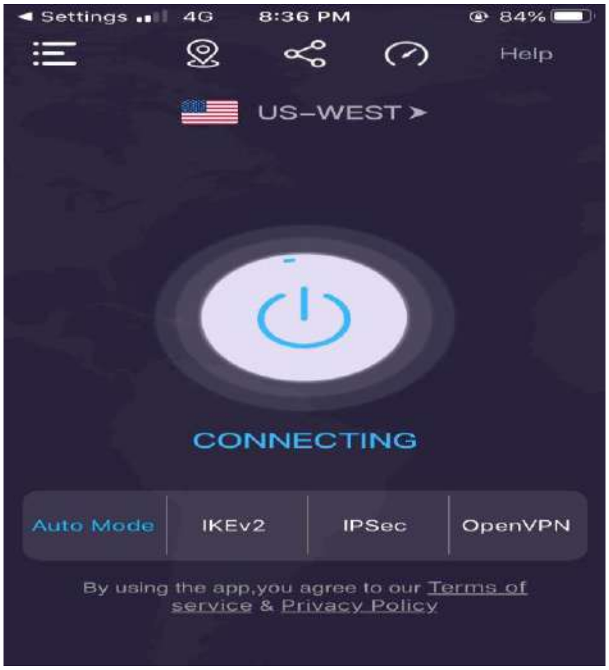


Figure 1.8: VPN application



By using the app,you agree to our Terms of service & Privacy Policy

Figure 1.9: Setting the VPN connection

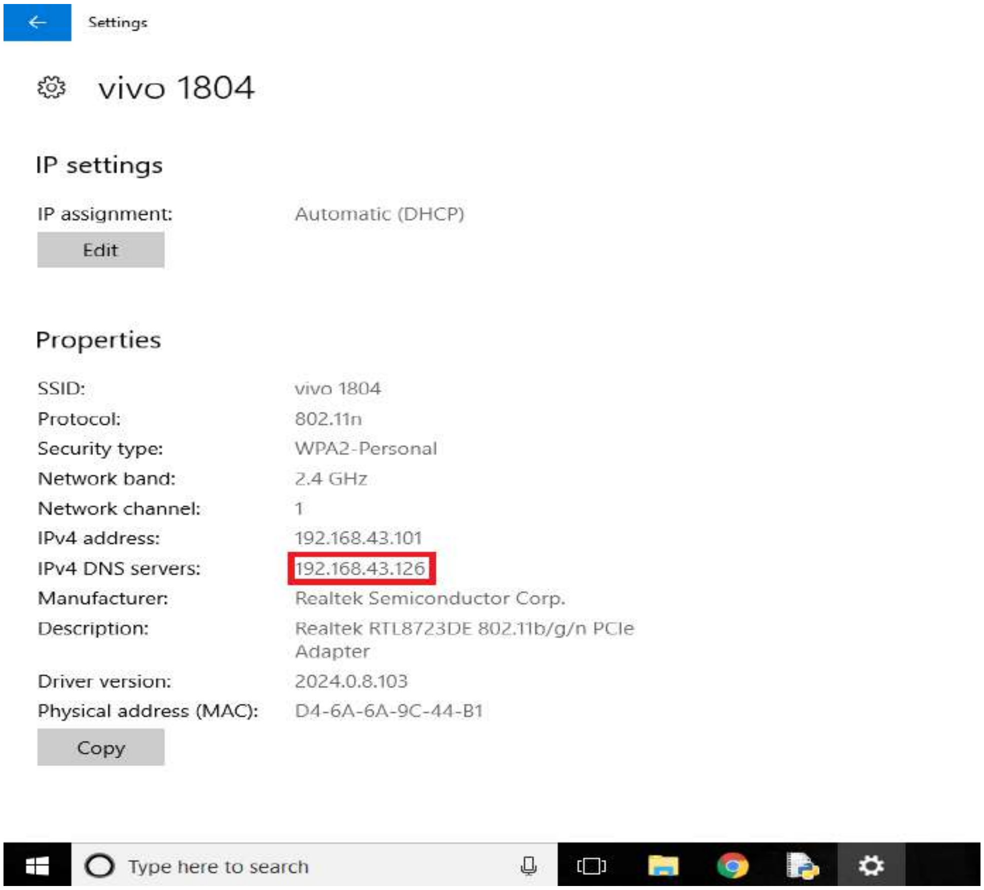
CHAPTER V

RESULTS AND CONCLUSION

RESULT

The virtual private network was able to hide the ip dns server address and thus, the device location, however the mac address was not hidden.

IN ANDROID SHARING OF HOTSPOT WITH LAPTOP
WITHOUT USING VPN: (shown in Figure 1.10)



vivo 1804

IP settings

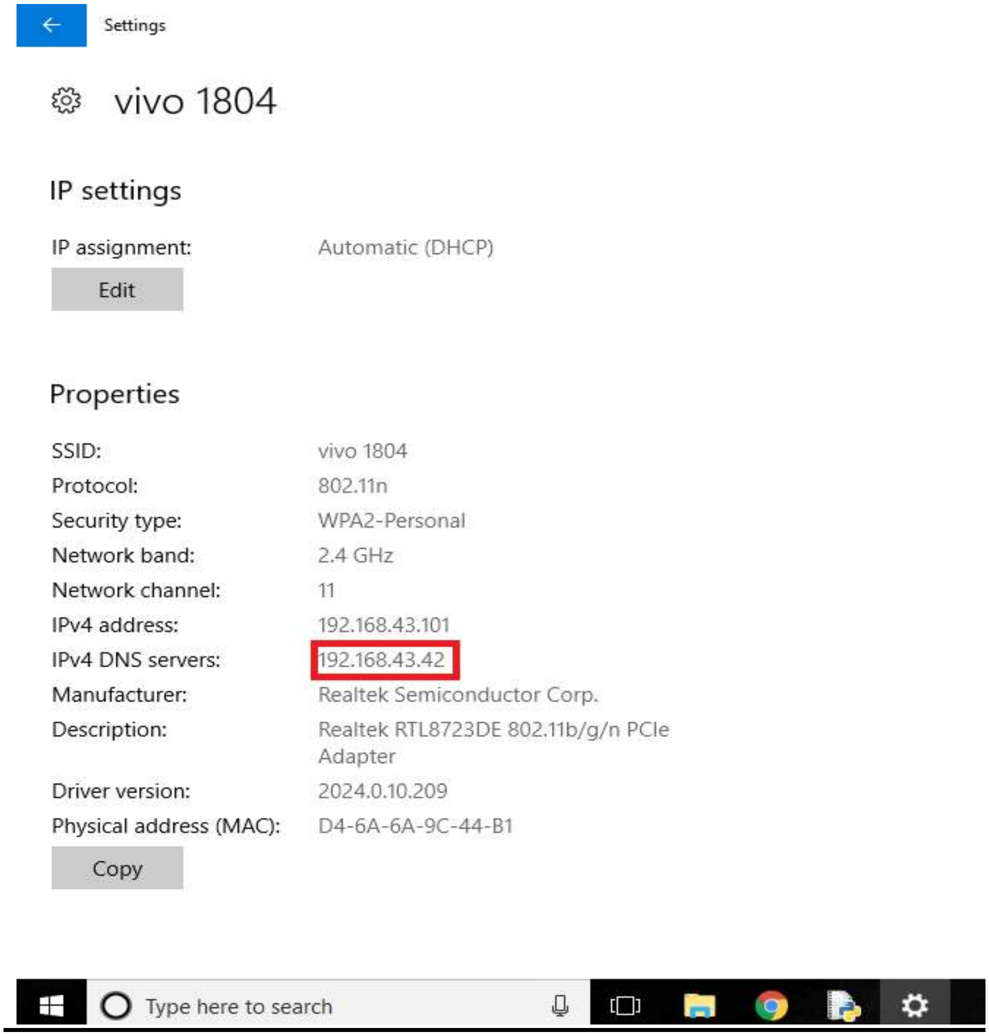
IP assignment:	Automatic (DHCP)

Properties

SSID:	vivo 1804
Protocol:	802.11n
Security type:	WPA2-Personal
Network band:	2.4 GHz
Network channel:	1
IPv4 address:	192.168.43.101
IPv4 DNS servers:	192.168.43.126
Manufacturer:	Realtek Semiconductor Corp.
Description:	Realtek RTL8723DE 802.11b/g/n PCIe Adapter
Driver version:	2024.0.8.103
Physical address (MAC):	D4-6A-6A-9C-44-B1

Figure 1.10: IP settings without the use of VPN

WITH THE USE OF VPN: (shown in Figure 1.11)



vivo 1804

IP settings

IP assignment: Automatic (DHCP)

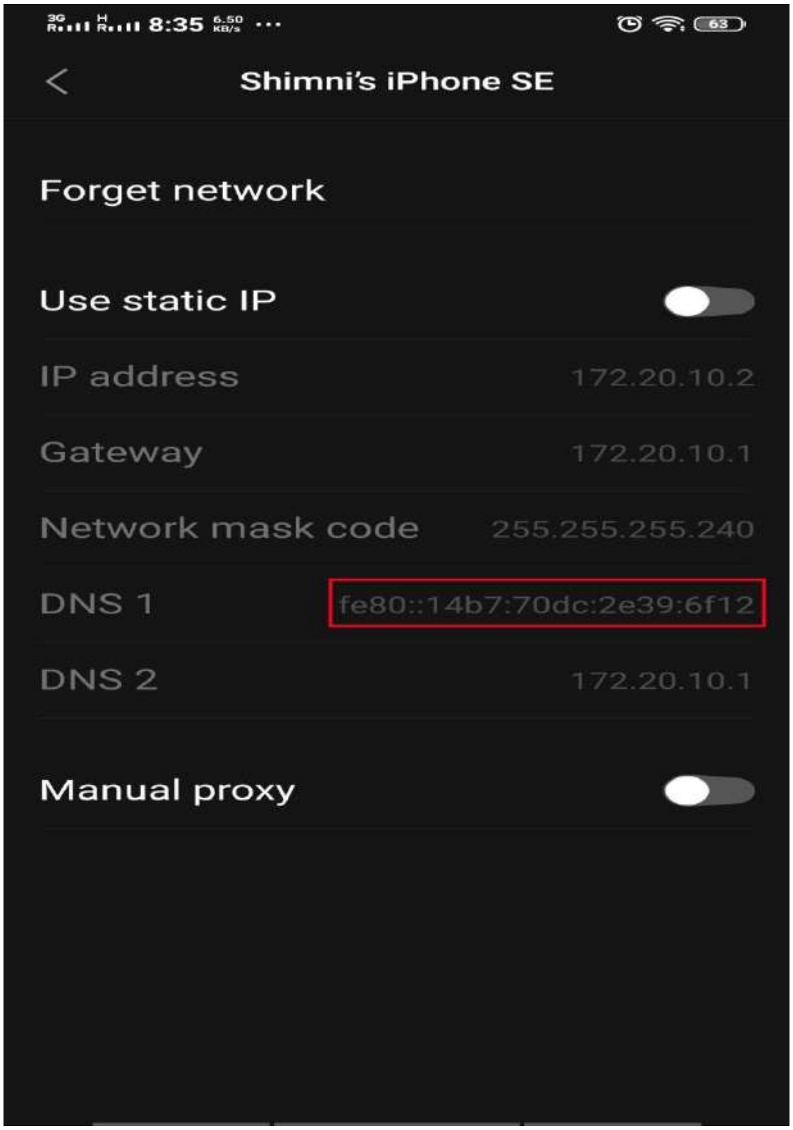
Properties

SSID:	vivo 1804
Protocol:	802.11n
Security type:	WPA2-Personal
Network band:	2.4 GHz
Network channel:	11
IPv4 address:	192.168.43.101
IPv4 DNS servers:	192.168.43.42
Manufacturer:	Realtek Semiconductor Corp.
Description:	Realtek RTL8723DE 802.11b/g/n PCIe Adapter
Driver version:	2024.0.10.209
Physical address (MAC):	D4-6A-6A-9C-44-B1

Figure 1.11: IP settings when VPN is connected

IN iOS, SHARING OF HOTSPOT WITH ANDROID DEVICE

a) WITHOUT VPN



Shimni's iPhone SE

Forget network

Use static IP

IP address 172.20.10.2

Gateway 172.20.10.1

Network mask code 255.255.255.240

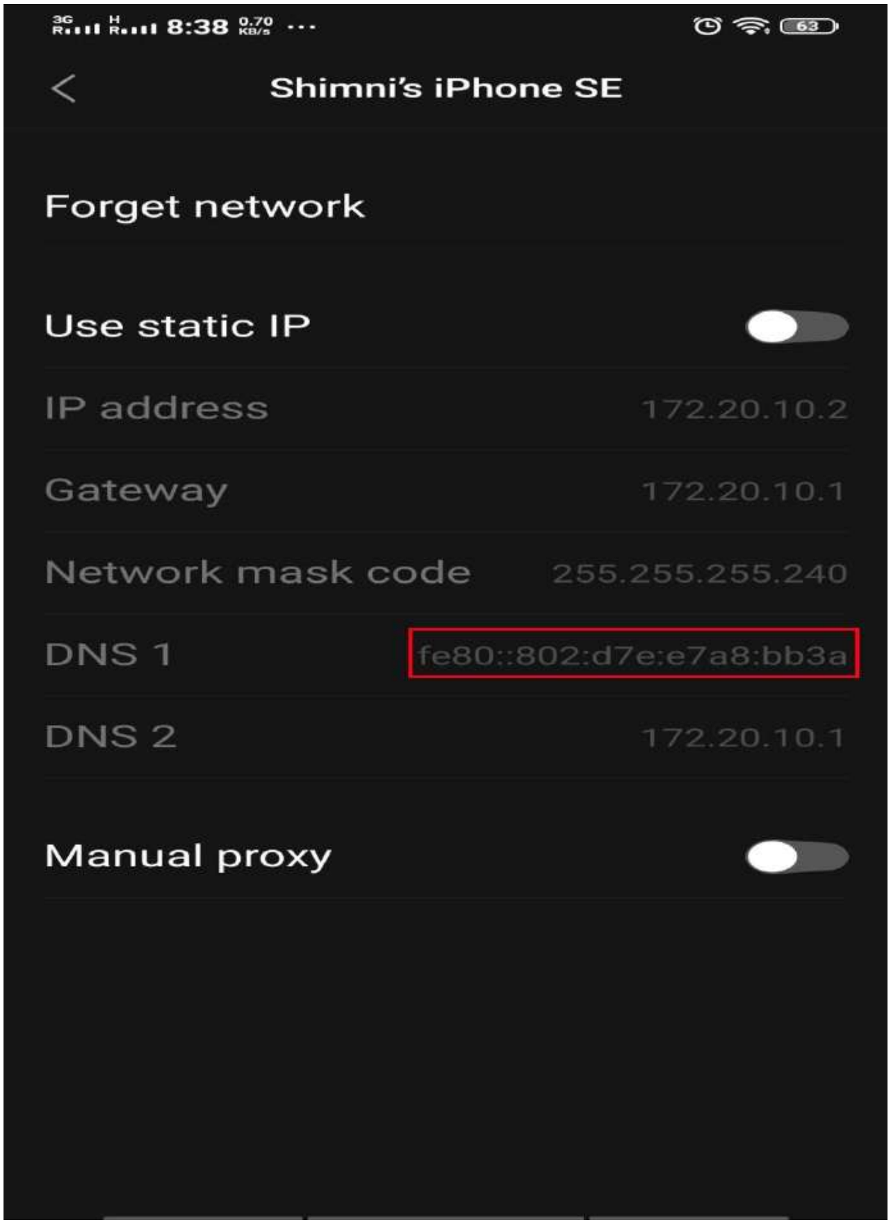
DNS 1 fe80::14b7:70dc:2e39:6f12

DNS 2 172.20.10.1

Manual proxy

Figure 1.12: Device without VPN

b) WITH VPN



Shimni's iPhone SE

Forget network

Use static IP

IP address 172.20.10.2

Gateway 172.20.10.1

Network mask code 255.255.255.240

DNS 1 fe80::802:d7e:e7a8:bb3a

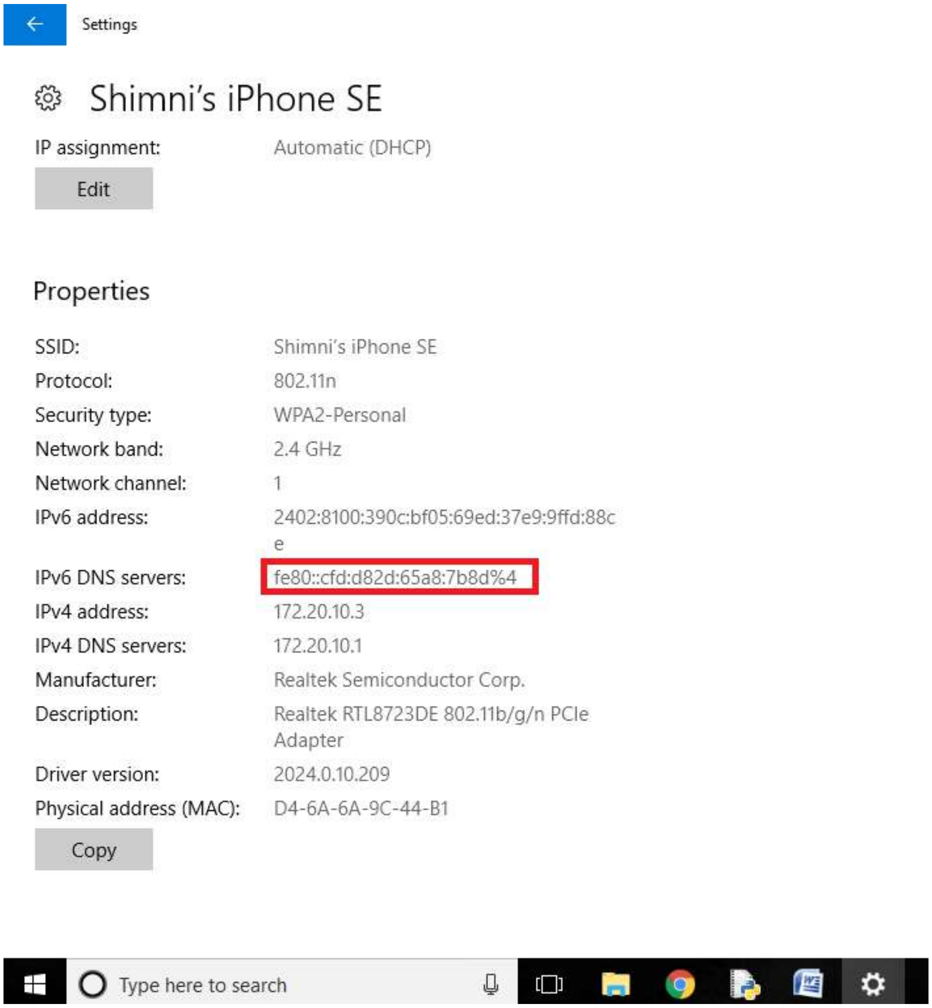
DNS 2 172.20.10.1

Manual proxy

Figure 1.13: Device when VPN is present

IN iOS, SHARING OF HOTSPOT WITH LAPTOP

a) WITHOUT VPN



Shimni’s iPhone SE

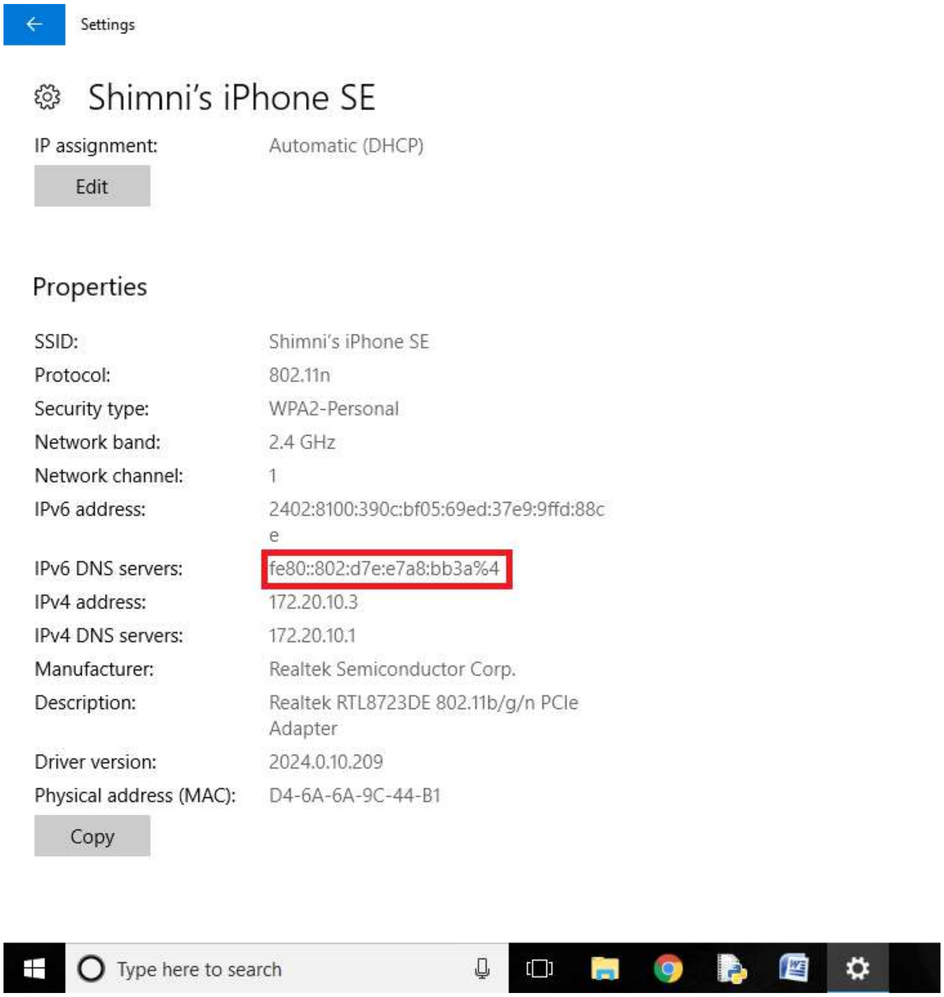
IP assignment:	Automatic (DHCP)

Properties

SSID:	Shimni’s iPhone SE
Protocol:	802.11n
Security type:	WPA2-Personal
Network band:	2.4 GHz
Network channel:	1
IPv6 address:	2402:8100:390c:bf05:69ed:37e9:9ffd:88ce
IPv6 DNS servers:	fe80::cfd:d82d:65a8:7b8d%4
IPv4 address:	172.20.10.3
IPv4 DNS servers:	172.20.10.1
Manufacturer:	Realtek Semiconductor Corp.
Description:	Realtek RTL8723DE 802.11b/g/n PCIe Adapter
Driver version:	2024.0.10.209
Physical address (MAC):	D4-6A-6A-9C-44-B1

Figure 1.14:IP settings of laptop without VPN

b) WITH VPN



Shimni’s iPhone SE

IP assignment:	Automatic (DHCP)

Properties

SSID:	Shimni’s iPhone SE
Protocol:	802.11n
Security type:	WPA2-Personal
Network band:	2.4 GHz
Network channel:	1
IPv6 address:	2402:8100:390c:bf05:69ed:37e9:9ffd:88ce
IPv6 DNS servers:	fe80::802:d7e:e7a8:bb3a%4
IPv4 address:	172.20.10.3
IPv4 DNS servers:	172.20.10.1
Manufacturer:	Realtek Semiconductor Corp.
Description:	Realtek RTL8723DE 802.11b/g/n PCIe Adapter
Driver version:	2024.0.10.209
Physical address (MAC):	D4-6A-6A-9C-44-B1

Figure 1.15: IP settings of laptop without VPN

CONCLUSION

- The ip addresses of both the devices were observed to be the same.
- Mobile hotspots let users remotely connect to the Internet without being dependent on possibly unsafe public Wi-Fi networks. With the ability to connect multiple devices to a single hotspot, these devices are an easy way to increase productivity.
- The VPN applications may be able to provide encryption to the data packets that are transmitted, however they are not able to hide the device information to a full extent.
- This can be considered as a vulnerability which the hackers may take up, to launch an attack and to keep the device under their supervision.
- At the same time, the vulnerability also provides an opportunity to understand the device to which we are connected via wi-fi
- It is better to share personal hotspots to a trusted devices only.
- The upcoming technology like cold tether or the idea of combining multiple hotspots may be able to overcome the vulnerability.

CHAPTER VI: REFERENCES

1. http://www.mypublicwifi.com/publicwifi/en/index.html
2. https://android.stackexchange.com/questions/194255/is-it-possible-to-share-a-vpn-connection-over-wifi-hotspot
3. http://cseweb.ucsd.edu/~voelker/pubs/hotspots-wmash03.pdf
4. https://support.hidemyass.com/hc/en-us/articles/207493567-Sharing-VPN-connection-via-Wifi-hotspot-Windows-
5. https://www.xda-developers.com/vpn-hotspot-share-vpn-connection/
6. https://en.wikipedia.org/wiki/Tethering
7. https://www.emerald.com/insight/content/doi/10.1108/info-05-2013-0033/full/html
8. https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network
9. https://www.webtitan.com/blog/wi-fi-security-threats-you-should-be-aware-of/
10. https://www.quora.com/How-do-I-spoof-MAC-address-in-Android
11. https://www.androidcentral.com/android-internet-tether
12. https://www.intel.in/content/www/in/en/tech-tips-and-tricks/what-is-a-hotspot.html
13. https://www.techadvisory.org/2018/04/how-to-boost-your-mobile-hotspot/
14. https://softstribe.com/android/top-10-best-vpn-android-apps-browse-internet-anonymously/
15. https://softstribe.com/android/android-101-connect-multiple-vpn-android/
16. https://computer.howstuffworks.com/vpn.htm
17. https://en.wikipedia.org/wiki/Virtual_private_network
18. https://www.windowscentral.com/how-manually-configure-vpn-windows-10
19. https://www.computerworld.com/article/2499772/how-to-use-a-smartphone-as-a-mobile-hotspot.html
20. https://www.vpnmentor.com/blog/vpn-protocol-comparison-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/
21. https://www.comparitech.com/vpn/protocols/

22. http://wndw.net/pdf/wndw3-en/wndw3-ebook.pdf
23. https://www.skyneel.com/use-android-phone-as-a-modem-to-run-internet-on-your-computer
24. https://www.microsoft.com/en-us/research/publication/cool-tether-energy-efficient-on-the-fly-wifi-hot-spots-using-mobile-phones/
25. https://www.microsoft.com/en-us/research/project/cool-tether/
26. https://www.comparitech.com/vpn/protocols/
27. https://bestvaluevpn.com/comparison-chart/vpn-app/?utm_campaign=ggls-en&gclid=EAIaIQobChMI36qR3KGL5wIVlw4rCh3Q4wD1EAAYAyAAEgKlh_D_BwE