1. **Title:**

|  |
| --- |
| **Encrypted Network Traffic Analysis for VPNs** |

1. **Short Rationale of FYP:**

|  |
| --- |
| The usage of VPNs is expanding as people become more concerned about their online privacy and security, as well as the desire to go around geo-restrictions and access region-specific material. **Controlling** **VPN** **use**, on the other hand, is critical for **preventing security concerns by monitoring and controlling encrypted traffic, protecting against possible misuse, optimizing network performance, and ensuring compliance with network policies and laws**. **Deep packet analysis is critical for comprehending network traffic** (Figure 1) since it inspects individual data packets, allowing for better security monitoring, threat detection, and network optimization. However, there has been little study towards identifying internal application activity via encrypted network traffic, particularly for VPNs. There is a dire need to research encryption solutions for today's cutting-edge network traffic for analysis and inspection.    Figure 1  The purpose of this research is to **look into the encrypted network traffic used by VPN providers to determine the traffic pattern, protocol identification, and participating servers**. The proposed methodology will capture traffic using a P4 Switch, as shown in Figure 2. Various VPNs will be installed on devices and linked to the internet through a wireless access point passing through switch. To filter out the corresponding apps, all internet traffic from the wireless access point will be routed through the P4 switch and information will be forwarded to the controller. Wireshark and other cutting-edge tools will be used to monitor encrypted data via trace file analysis for network traffic monitoring. The IP addresses, ports, packet lengths, and packet patterns will be utilized to identify the VPN and the exact VPN that is being used. It is worth mentioning that the IP addresses and ports are in plaintext, however the payloads are encrypted for the purpose of secrecy and privacy. The knowledge gathered from this study will aid in the **building of a Network Traffic Analysis for VPNs, as well as the ability to block VPN in a specific network.**  Figure 2: |

1. **Major Objectives:**

|  |
| --- |
| * Acquire a thorough comprehension of the analysis of encrypted network traffic. * The goal of this study is to look into the difficulties in examining network traffic that has been tunneled or encrypted. * Recognize and investigate the many applications and use cases for encrypted traffic analysis. |

1. **Outcomes of the FYP:**

|  |
| --- |
| * 1x high-quality publication * A straightforward encrypted network traffic analysis module capable of distinguishing between VPN and conventional traffic as well as particular VPN types. * A web interface that provides real-time traffic analysis and allows us to disable VPN connections in a specified network. |

1. **Major Equipment Required:**

|  |
| --- |
| * 2x Laptop (Available in NUST) * Wireshark, P4 Switch Image, and (Available in NUST) |

1. **Possibility of Commercialization:**

|  |
| --- |
| * Any organization with the necessary resources may achieve a VPN-free network environment by extending the proof of concept under the proposed study into a real-world application. |

1. **End-user(s) Keen to Adopt the FYP Results:**

|  |
| --- |
| * The suggested encrypted analyzer module may be placed at the network administrator level in an organization to identify VPN activity in the network and give the ability to stop the VPN. |