**COMP 7003**

**Introduction to Information and Network Security**

*Assignment-02*

*User Guide*

##### Anmol Mittal A01397754

##### February 2nd, 2025

##### Course Reference Number (CRN): 91662

[**Purpose** 3](#_Toc189346319)

[**Installation** 3](#_Toc189346320)

[Building 3](#_Toc189346321)

[Running 3](#_Toc189346322)

[**Command Line Arguments** 3](#_Toc189346323)

[main.py 3](#_Toc189346324)

[**Examples** 4](#_Toc189346325)

# **Purpose**

The purpose of the program is to capture and analyze network traffic at the packet level using Python and Scapy. It will filter packets by protocol (Ethernet, IPv4, ICMP, TCP, UDP, DNS, IPv6, ICMPv6), convert raw packet data into hexadecimal dumps, and parse the packet headers to extract and display key fields such as source/destination MAC and IP addresses, protocol-specific details, and port numbers. The program aims to provide a clear, structured, and human-readable output of packet information.

# **Installation**

Navigate to <https://learn.bcit.ca>. Download COMP7003-assign02-v1.zip and Extract the contents.

## Requirements

Need Scapy installed.

## Building

No building required

## Running

sudo python3 main.py -i <interface> -f <filter> -c <count>

# **Command Line Arguments**

The following configuration values can be set in <file>:

### main.py

|  |  |
| --- | --- |
| **Variable** | **Purpose** |
| <-i> or <--interface> | Specifies the network interface to capture packets on. (Default: any) |
| <-f> or <--filter> | Specifies the BPF to apply. Common filters include tcp, udp, icmp, arp, ip, ip6, icmp6, and dns. |
| <-c> or <--count> | Specifies the number of packets to capture. (Default: 1) |

# **Examples**

|  |
| --- |
| main.py |
|  |