**Task 05**

**Network Packet Analyzer**

**Develop a packet sniffer tool that captures and analyzes network packets. Display relevant information such as source and destination IP addresses, protocols, and payload data. Ensure the ethical use of the tool for educational purposes.**

## **📘 Introduction**

A **packet sniffer** (also known as a **network analyzer** or **protocol analyzer**) is a tool that captures, interprets, and logs packets of data that travel across a network. It can be used for **network diagnostics, performance analysis, educational purposes**, and security auditing.

This project presents a **Packet Sniffer Tool built using Python and the Scapy library**. It enables real-time analysis of packets, showing details like **source and destination IPs**, **protocol types**, and **payload contents**.

⚠️ **Disclaimer**: This tool is developed strictly for educational and authorized use. Unauthorized sniffing of network traffic may violate privacy laws.

## ⚙️ How the Tool Works

The tool performs the following steps:

1. Initializes Scapy to **sniff packets** from the system’s active network interface.
2. For each captured packet:
   * Extracts **source and destination IP addresses**.
   * Identifies the **protocol** (TCP/UDP).
   * Displays **port numbers**.
   * Decodes and prints the **payload** if available.
3. Runs continuously until manually stopped (e.g., using CTRL+C).

## 🧠 Python Code (Packet Sniffer)

### 📦 Step 1: Install Scapy

pip install scapy

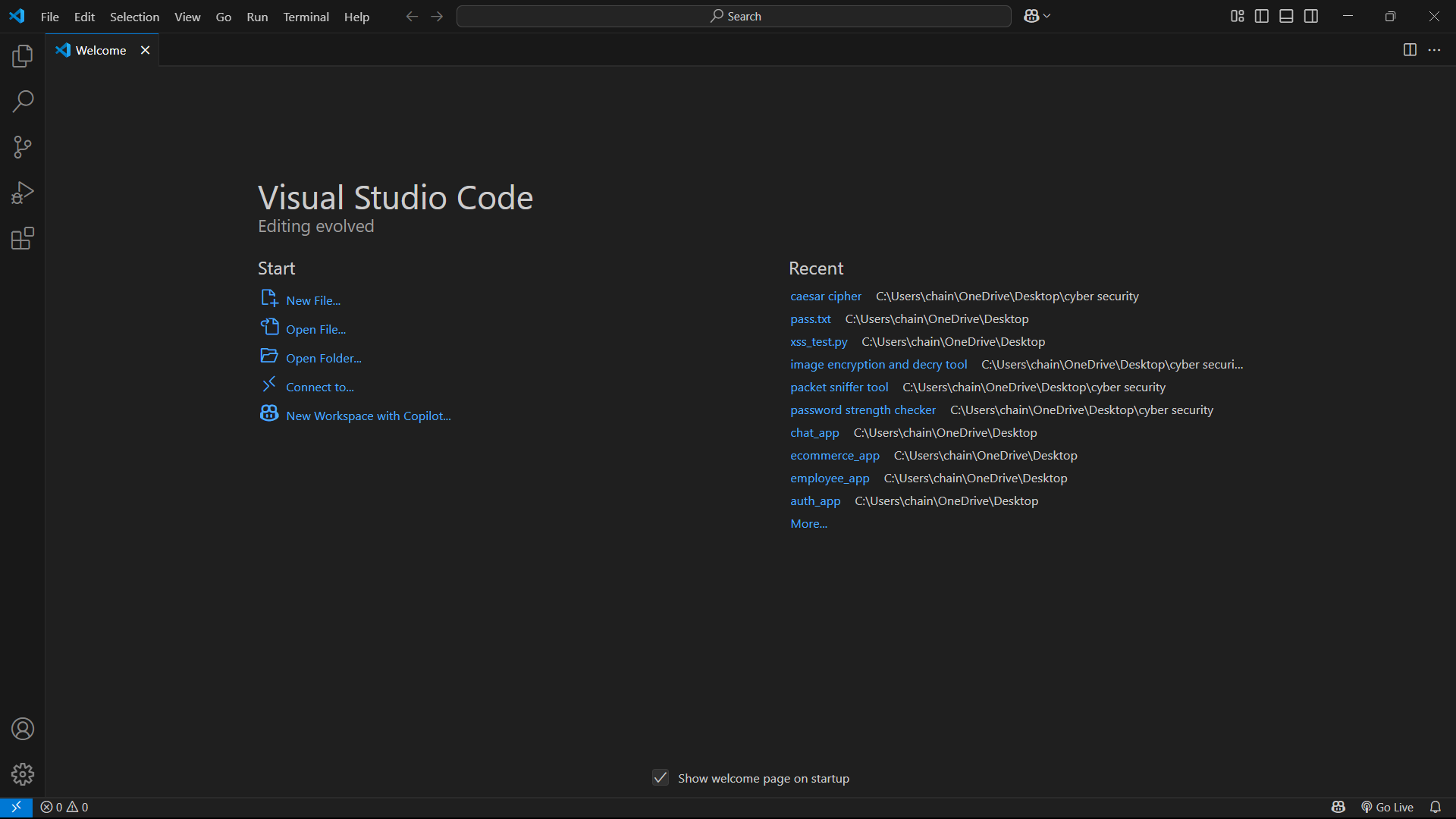
### **🧾 Step 2: Python Script**

**Implementation of code in Python**

**Steps: -**

1. Choose a code editor or IDE as per your choice.
2. Install and set up **VS code.**

Download: Visit <https://code.visualstudio.com/> and install VS Code.



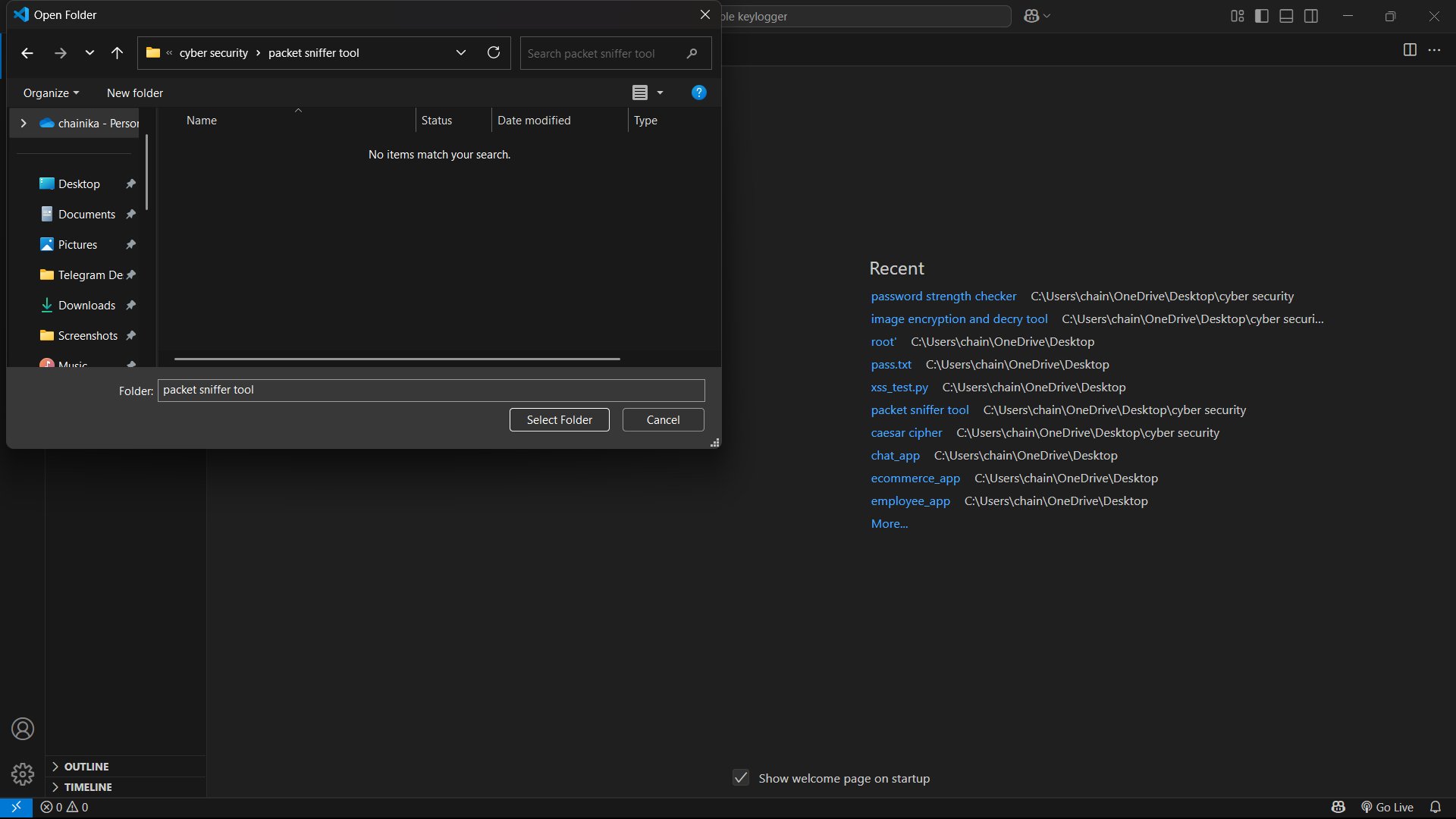
Go to extension tab (ctrl+ shift+ x) and search for Python. Click install on the official Microsoft Python extension.

Choose python interpreter (I have selected Python 3.12.7)

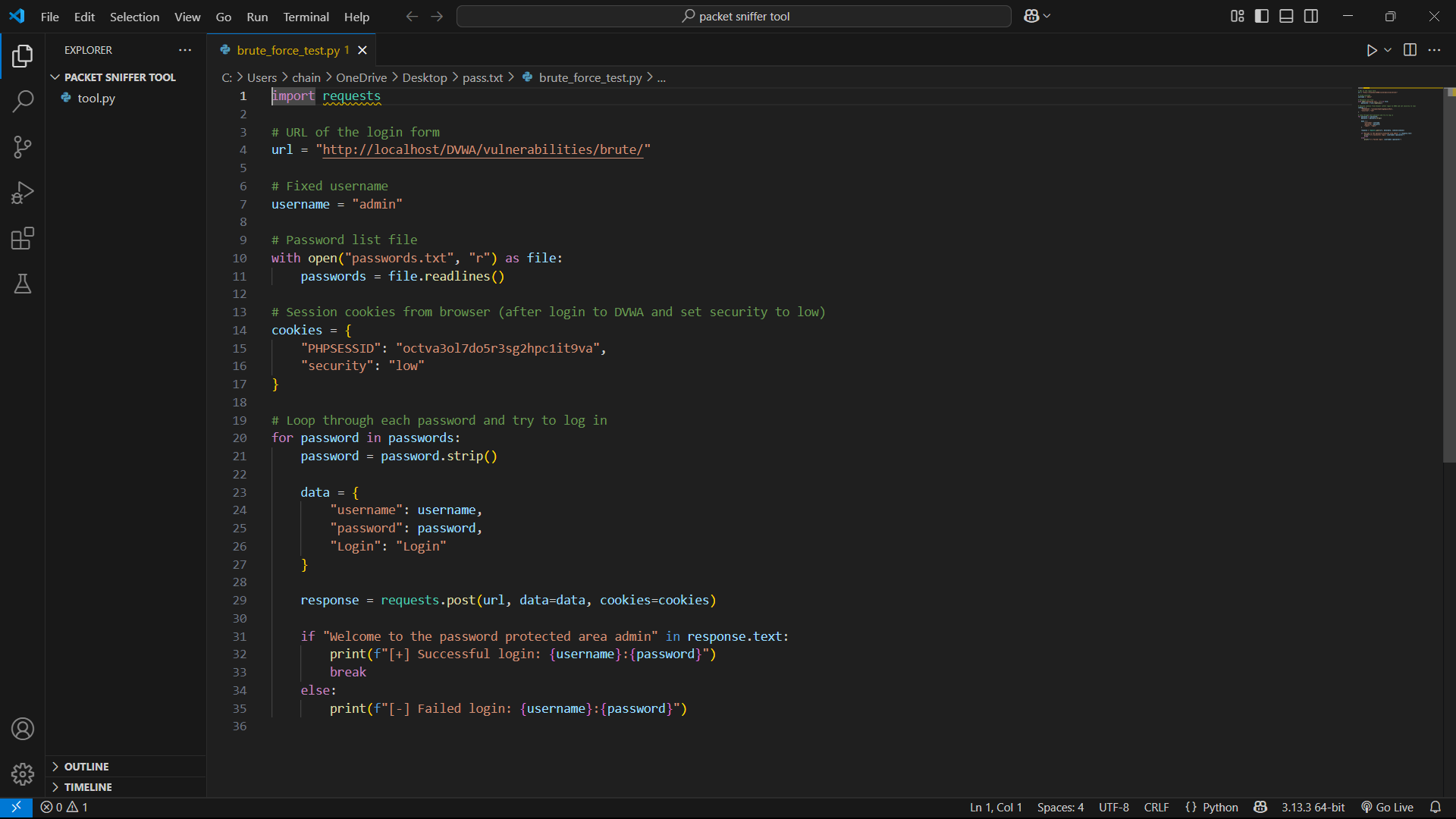
1. Create and save a python file (file having extension .py)

In VS Code: File : New File.

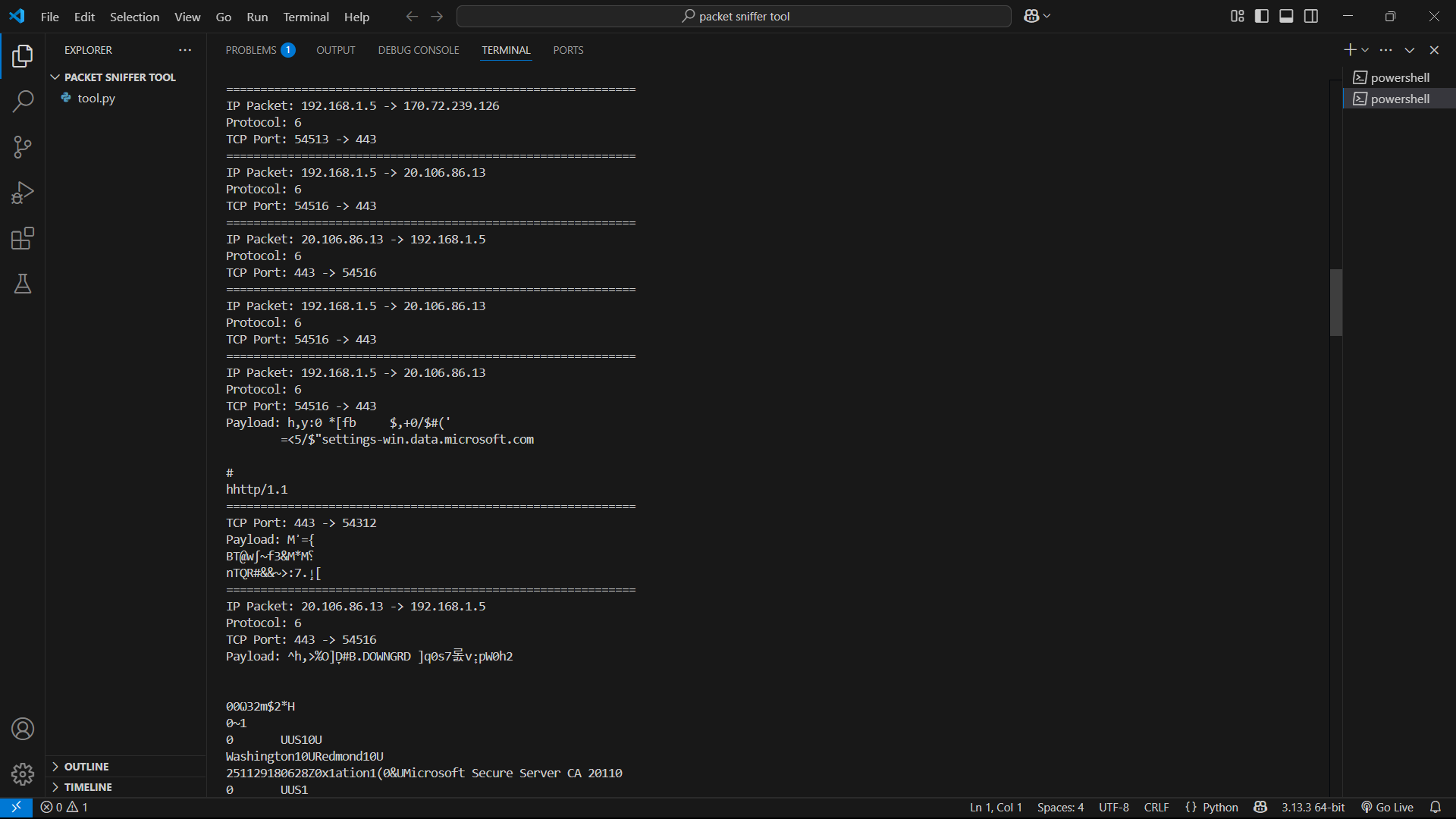
And, Save the file extension .py



1. Initiate with writing your program:



1. Then Run the program in the terminal:



Successful running of program with the result shows the correct program.

## ****🔐 Ethical and Legal Considerations****

* **Use only on networks you own or have explicit permission to monitor**.
* **Never capture data from public or third-party networks**.
* Use for:
  + ✅ Network troubleshooting
  + ✅ Educational demonstrations
  + ✅ Security research (in lab settings)
* Avoid:
  + ❌ Intercepting private data without consent
  + ❌ Misuse for spying, credential theft, or surveillance

## 🎯 Significance of the Tool

* 📚 **Educational Value**: Excellent for learning how real network traffic works.
* 🛠 **Diagnostic Utility**: Can be used to detect misrouted traffic, dropped connections, and unusual data flow.
* 🔐 **Security Awareness**: Demonstrates how easily unencrypted traffic can be intercepted, underscoring the importance of HTTPS and VPNs.
* 💡 **Foundation for Advanced Tools**: This project is a base for building more advanced tools like firewalls, intrusion detection systems (IDS), or protocol analyzers.

## ✅ Conclusion

This Packet Sniffer Tool demonstrates how Python and Scapy can be used to capture and analyze real-time network traffic. It is a valuable educational project for understanding **network protocols**, **packet structures**, and the **importance of network security**. While powerful, such tools must be used **ethically and legally**, strictly for authorized purposes.

**Presented by: - Chainika Dongre Date: - 19 May 2025**