MIT-WPU

॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Dr. Vishwanath Karad
MIT WORLD PEACE
UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

School of Computer Engineering and Technology
Academic Year: 2023-2024 Sem V

Digital Forensics and Investigation

Lab Assignment : 02

Title: Log Capturing using a wireless router. Perform suitable event correlation and analysis of network traffic.

Prepared By

Saurabh Jitendra Jadhav
Roll No: PA12
Batch A1
September 8,2023

Aim: To capture a wifi router log and to investigate it

Objective:

1. **Configure Log Capturing:** To set up a wireless router for capturing network logs, enabling essential logging features, and directing log data to a central location for analysis.
2. **Capture Network Traffic:** To capture network traffic using packet capture tools such as Wireshark, allowing for the collection of raw network data.
3. **Analyze Network Logs**: To employ log analysis tools and techniques to interpret and extract meaningful information from the captured network logs.

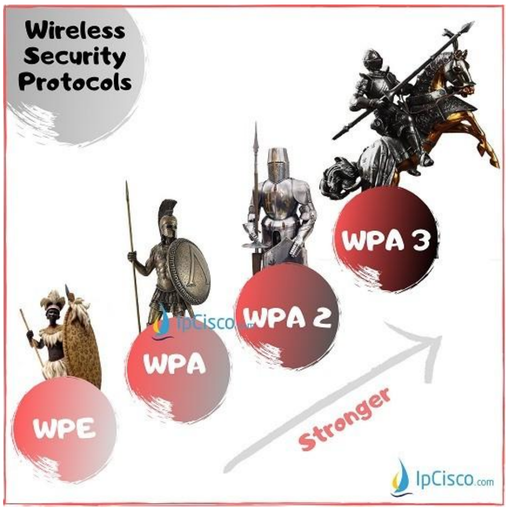
Theory:

Wireless Router:

Wireless Router

A wireless router is a network device that combines the functions of a traditional wired router with wireless access points. It enables wireless communication between devices (like laptops, smartphones, tablets) and a wired network (typically connected to the internet through a broadband modem). A wireless router allows devices to connect to the network without physical cables, providing flexibility and convenience for users. It often includes features like firewall protection, DHCP (Dynamic Host Configuration Protocol) for IP address assignment, and NAT (Network Address Translation) for routing traffic between the local network and the internet.

Wireless Security:



Wireless security protocol

Wireless security refers to measures and protocols implemented to protect wireless networks from unauthorized access, data breaches, and cyberattacks. Securing a wireless network is essential to prevent unauthorized users from connecting to the network and eavesdropping on data transmissions. Common wireless security mechanisms include encryption (like WPA and WPA2), authentication methods (like WEP keys and passwords), and network isolation (e.g., creating separate guest networks).

WPA (Wi-Fi Protected Access):

WPA, or Wi-Fi Protected Access, is a security protocol designed to secure wireless networks. There are two primary versions: WPA and WPA2. WPA addresses vulnerabilities in the earlier WEP (Wired Equivalent Privacy) protocol. It uses stronger encryption and authentication methods to protect wireless communications. WPA2 is an improved version of WPA and is considered more secure. It uses the AES (Advanced Encryption Standard) encryption algorithm, making it highly resistant to attacks.

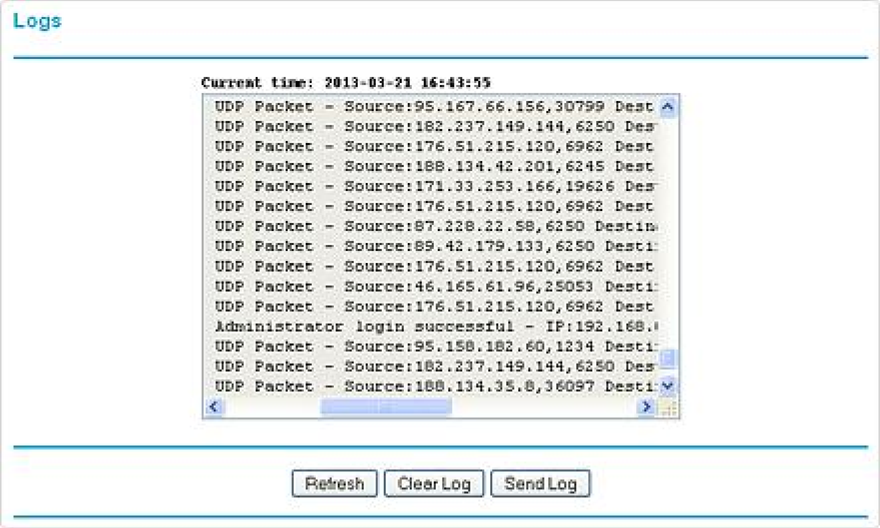
802.11b:

802.11b is a wireless networking standard that operates in the 2.4 GHz frequency band. It was one of the earliest Wi-Fi standards and provides a maximum data rate of up to 11 Mbps (megabits per second). 802.11b is considered relatively slow compared to later standards like 802.11g and 802.11n but is still used in some legacy devices and networks.

802.11g:

802.11g is another wireless networking standard that operates in the 2.4 GHz frequency band. It offers faster data rates compared to 802.11b, with a maximum rate of 54 Mbps. 802.11g is backward-compatible with 802.11b devices, making it a popular choice for upgrading older networks.

Logs:

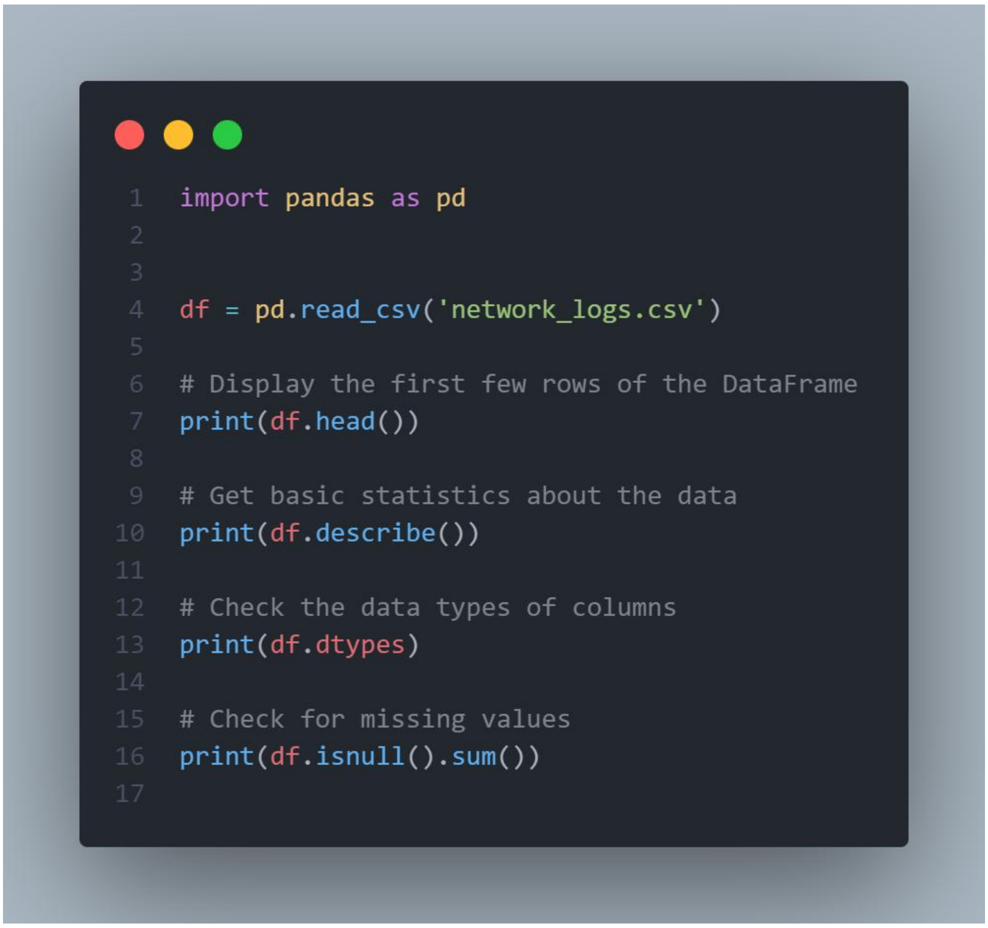


```
Current time: 2013-03-21 16:43:55
UDP Packet - Source:95.167.66.156,30799 Dest
UDP Packet - Source:182.237.149.144,6250 Des
UDP Packet - Source:176.51.215.120,6962 Dest
UDP Packet - Source:188.134.42.201,6245 Dest
UDP Packet - Source:171.33.253.166,19626 Des
UDP Packet - Source:176.51.215.120,6962 Dest
UDP Packet - Source:87.228.22.58,6250 Destin
UDP Packet - Source:89.42.179.133,6250 Desti
UDP Packet - Source:176.51.215.120,6962 Dest
UDP Packet - Source:46.165.61.96,25053 Desti
UDP Packet - Source:176.51.215.120,6962 Dest
Administrator login successful - IP:192.168.
UDP Packet - Source:95.158.182.60,1234 Desti
UDP Packet - Source:182.237.149.144,6250 Des
UDP Packet - Source:188.134.35.8,36097 Desti
```

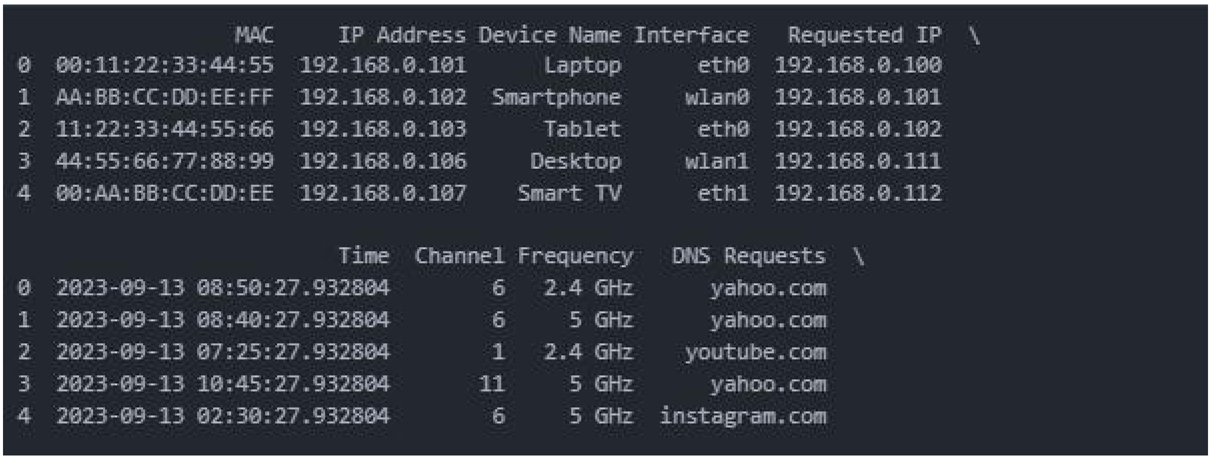
Wifi router Logs

Logs are records or files generated by computer systems and network devices to document various events and activities. In the context of networking and cybersecurity, logs are crucial for monitoring and troubleshooting. They provide a detailed history of system and network events, such as login attempts, network traffic, system errors, and security incidents. Logs are used for various purposes, including security analysis, compliance auditing, and debugging. Log data can be captured and stored on devices like routers, servers, and security appliances, and it is often reviewed and analyzed by IT professionals and security experts to detect and respond to anomalies, threats, and breaches.

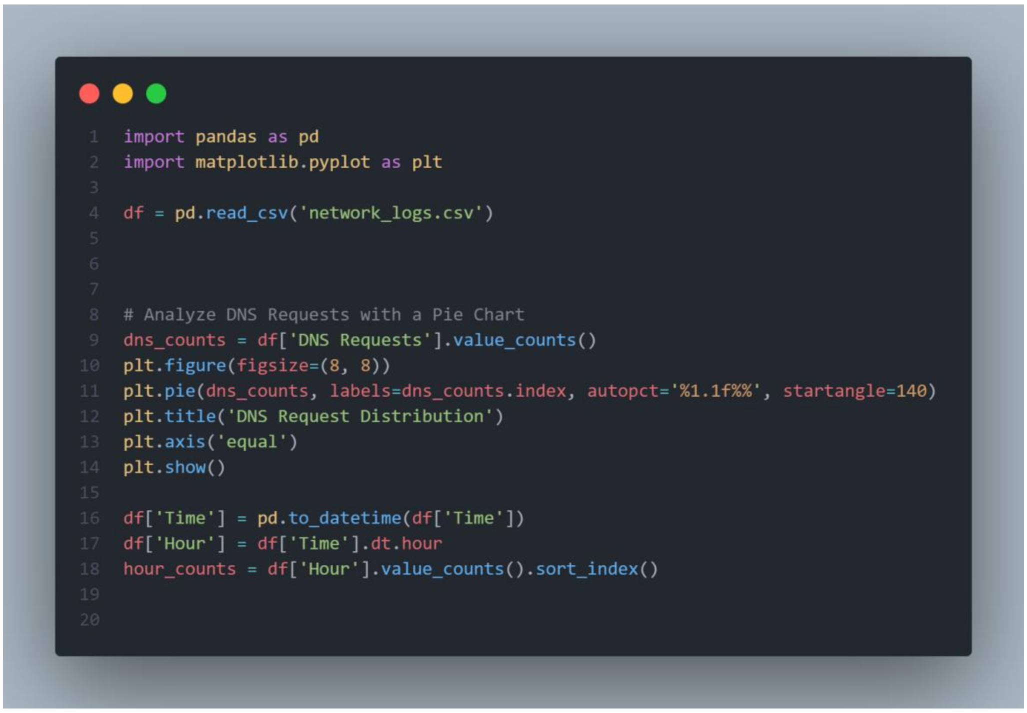
Implementation:



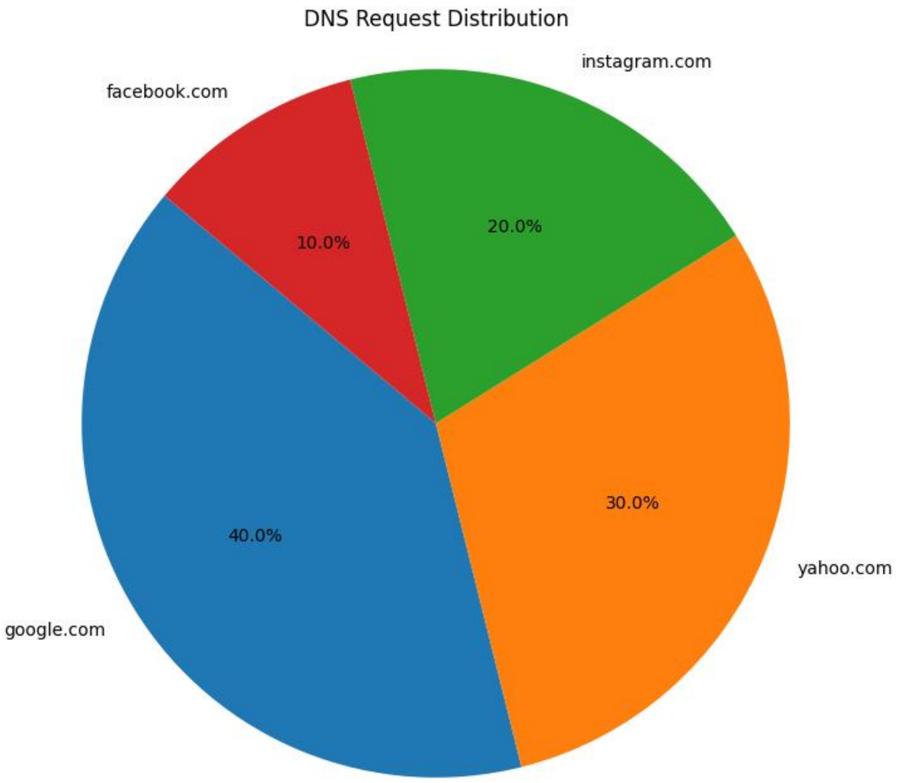
```python
import pandas as pd


df = pd.read_csv('network_logs.csv')

# Display the first few rows of the DataFrame
print(df.head())

# Get basic statistics about the data
print(df.describe())

# Check the data types of columns
print(df.dtypes)

# Check for missing values
print(df.isnull().sum())

```

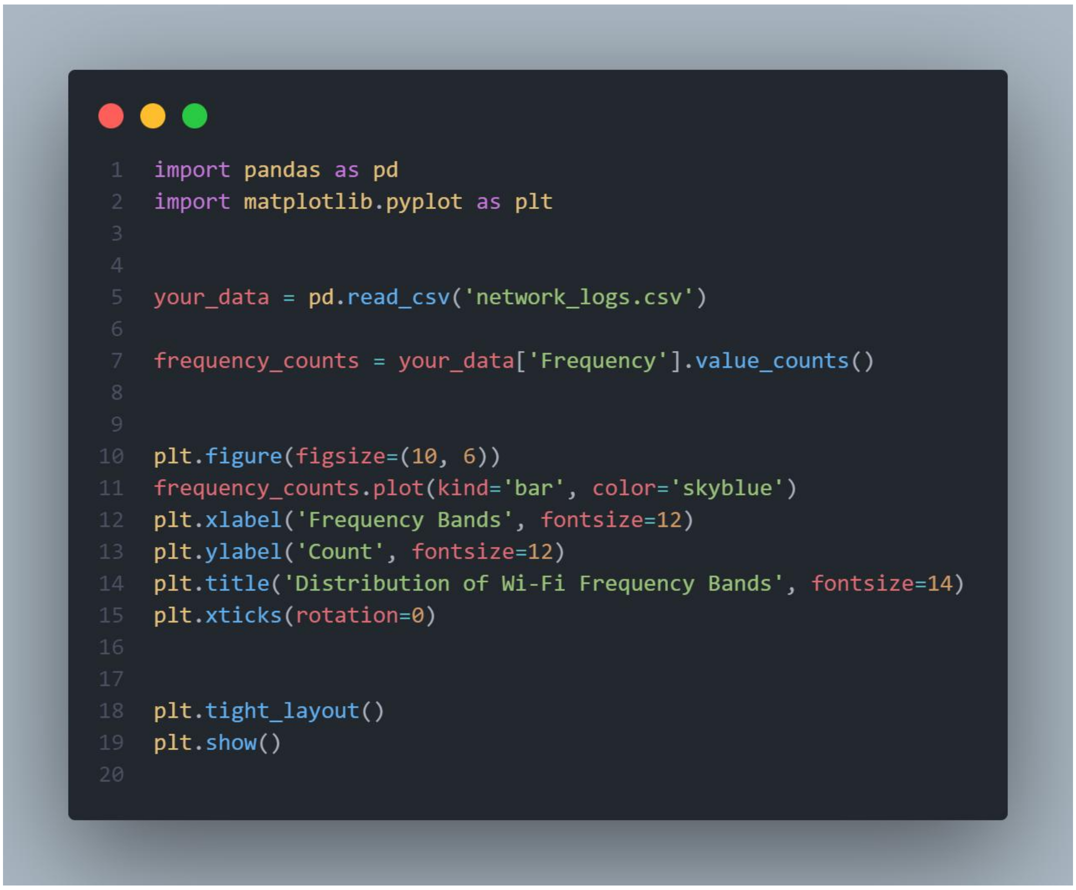


```
                 MAC     IP Address Device Name Interface   Requested IP  \
0  00:11:22:33:44:55  192.168.0.101      Laptop      eth0  192.168.0.100
1  AA:BB:CC:DD:EE:FF  192.168.0.102  Smartphone     wlan0  192.168.0.101
2  11:22:33:44:55:66  192.168.0.103      Tablet      eth0  192.168.0.102
3  44:55:66:77:88:99  192.168.0.106     Desktop     wlan1  192.168.0.111
4  00:AA:BB:CC:DD:EE  192.168.0.107    Smart TV      eth1  192.168.0.112

                         Time  Channel Frequency   DNS Requests  \
0  2023-09-13 08:50:27.932804        6   2.4 GHz      yahoo.com
1  2023-09-13 08:40:27.932804        6     5 GHz      yahoo.com
2  2023-09-13 07:25:27.932804        1   2.4 GHz    youtube.com
3  2023-09-13 10:45:27.932804       11     5 GHz      yahoo.com
4  2023-09-13 02:30:27.932804        6     5 GHz  instagram.com
```



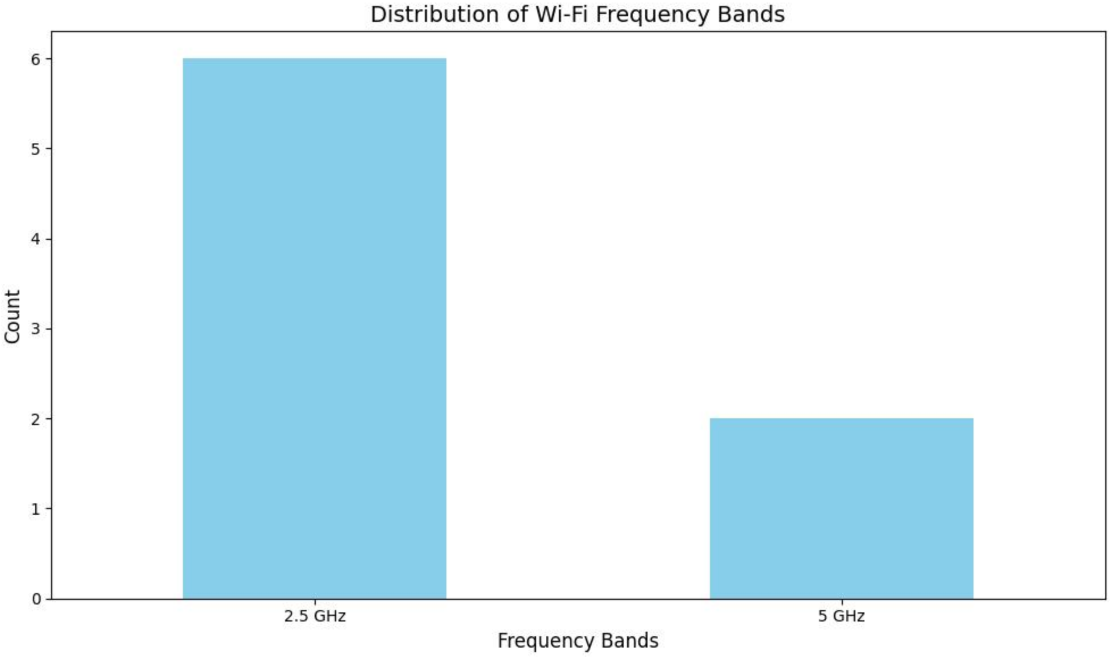
```python
import pandas as pd
import matplotlib.pyplot as plt

df = pd.read_csv('network_logs.csv')



# Analyze DNS Requests with a Pie Chart
dns_counts = df['DNS Requests'].value_counts()
plt.figure(figsize=(8, 8))
plt.pie(dns_counts, labels=dns_counts.index, autopct='%1.1f%%', startangle=140)
plt.title('DNS Request Distribution')
plt.axis('equal')
plt.show()

df['Time'] = pd.to_datetime(df['Time'])
df['Hour'] = df['Time'].dt.hour
hour_counts = df['Hour'].value_counts().sort_index()
```

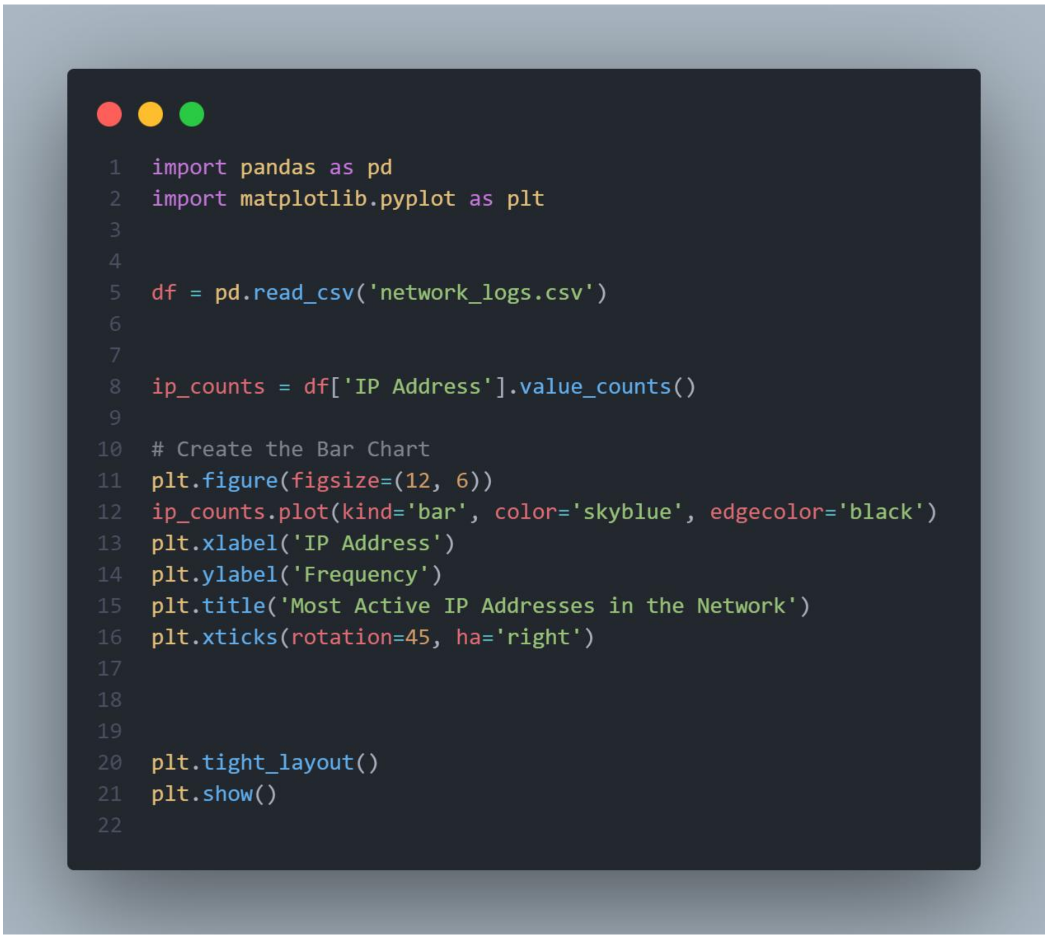




```python
import pandas as pd
import matplotlib.pyplot as plt


your_data = pd.read_csv('network_logs.csv')

frequency_counts = your_data['Frequency'].value_counts()


plt.figure(figsize=(10, 6))
frequency_counts.plot(kind='bar', color='skyblue')
plt.xlabel('Frequency Bands', fontsize=12)
plt.ylabel('Count', fontsize=12)
plt.title('Distribution of Wi-Fi Frequency Bands', fontsize=14)
plt.xticks(rotation=0)


plt.tight_layout()
plt.show()

```

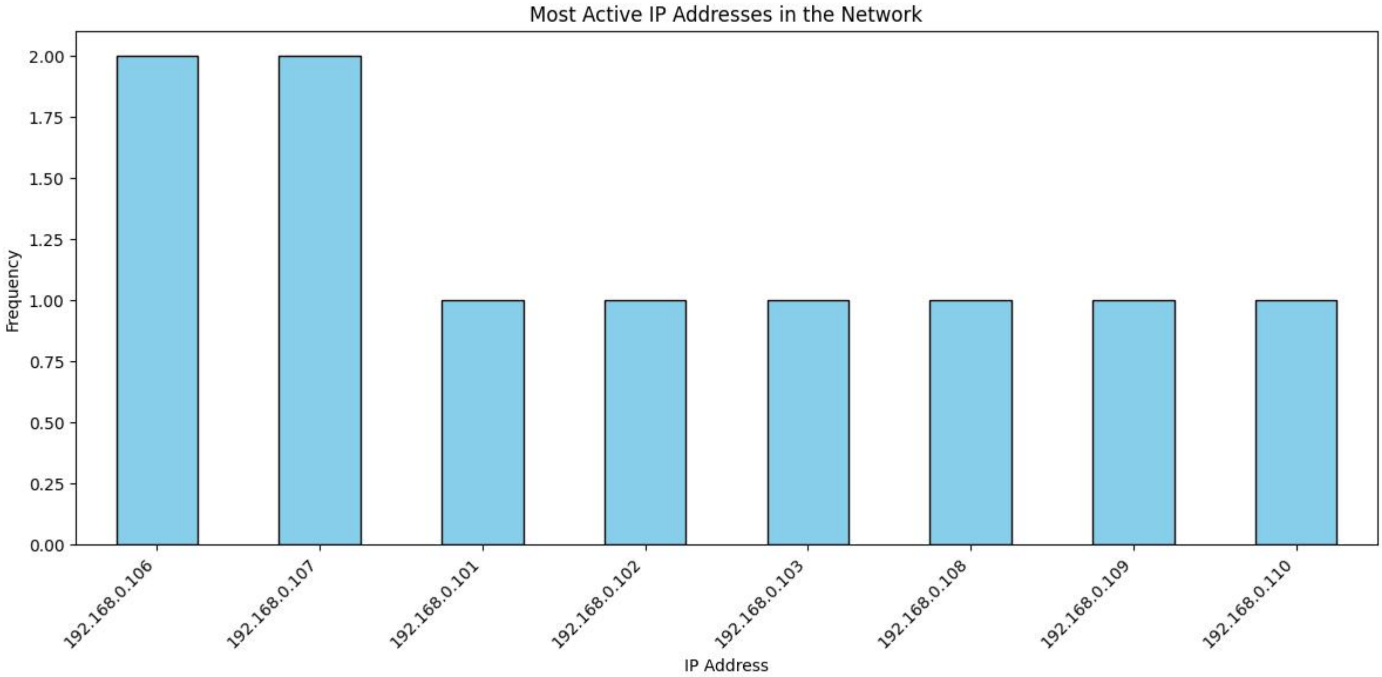
Output:-

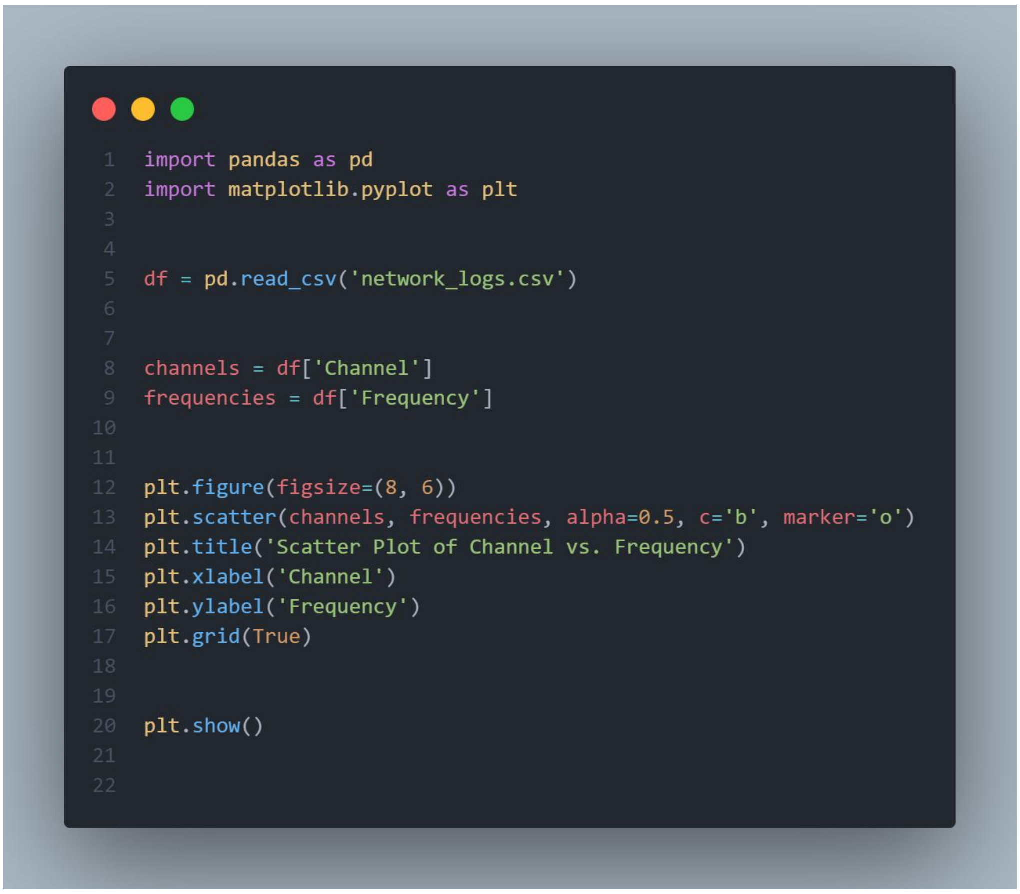




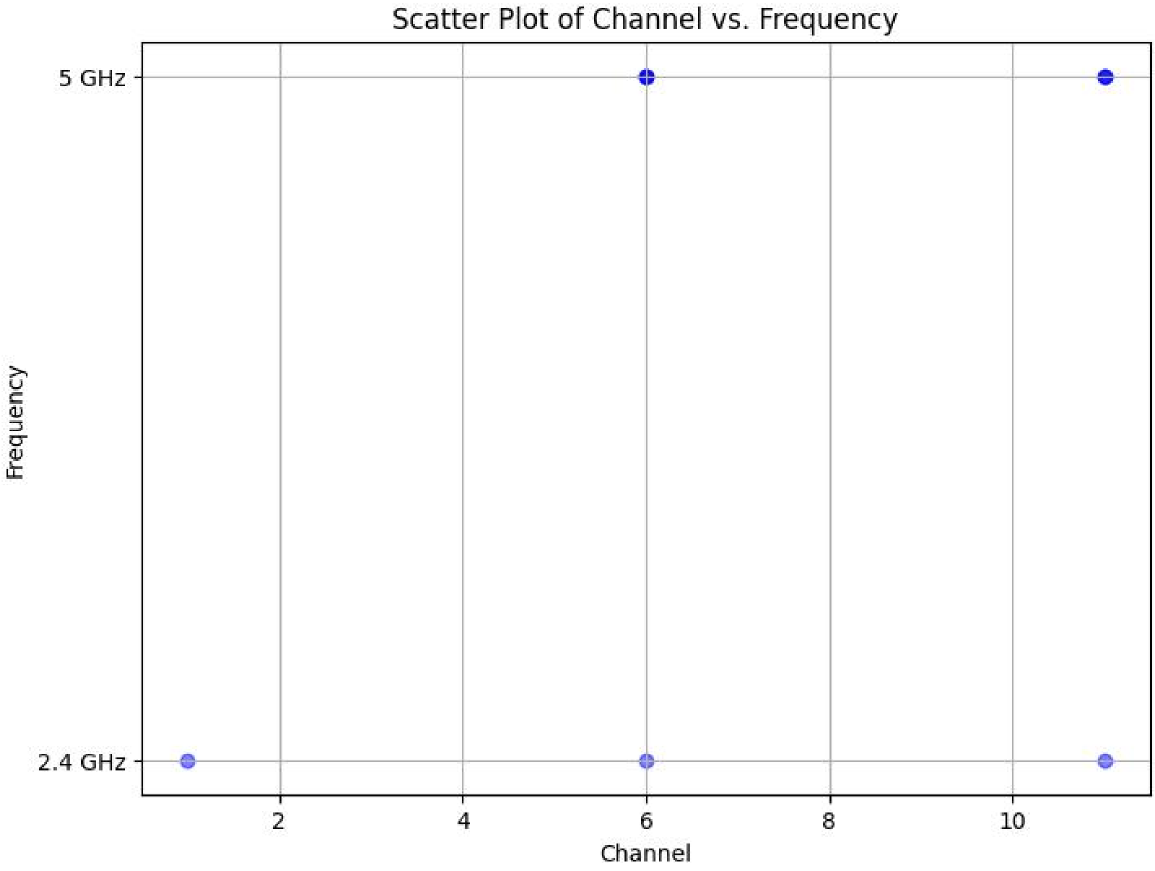
```python
import pandas as pd
import matplotlib.pyplot as plt


df = pd.read_csv('network_logs.csv')


ip_counts = df['IP Address'].value_counts()

# Create the Bar Chart
plt.figure(figsize=(12, 6))
ip_counts.plot(kind='bar', color='skyblue', edgecolor='black')
plt.xlabel('IP Address')
plt.ylabel('Frequency')
plt.title('Most Active IP Addresses in the Network')
plt.xticks(rotation=45, ha='right')



plt.tight_layout()
plt.show()

```

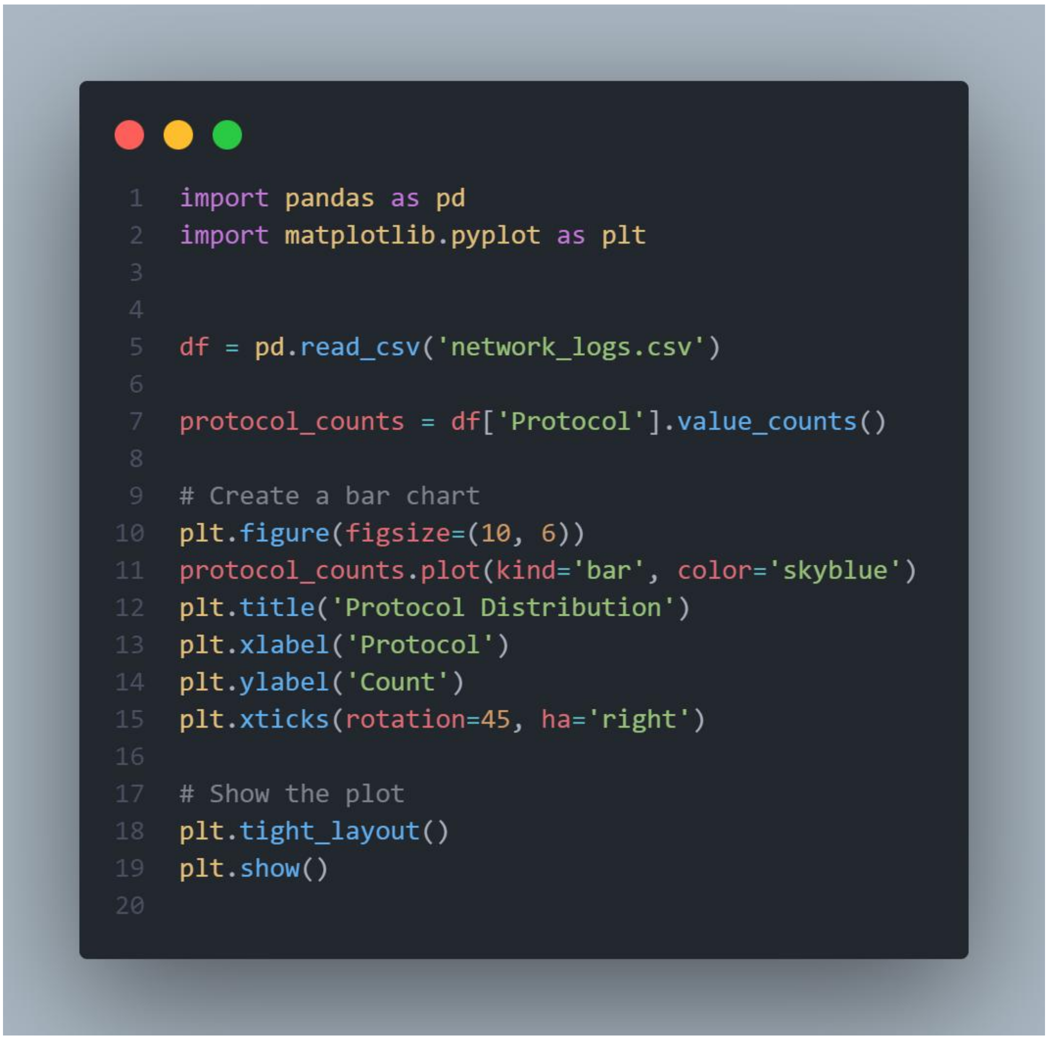
Output:-



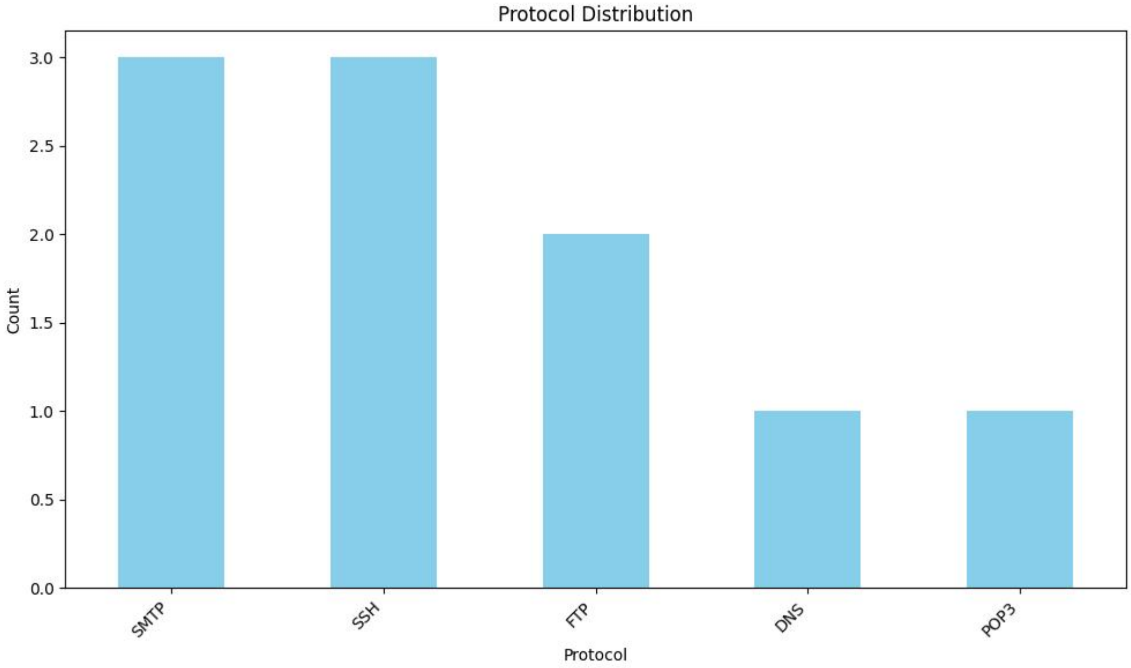


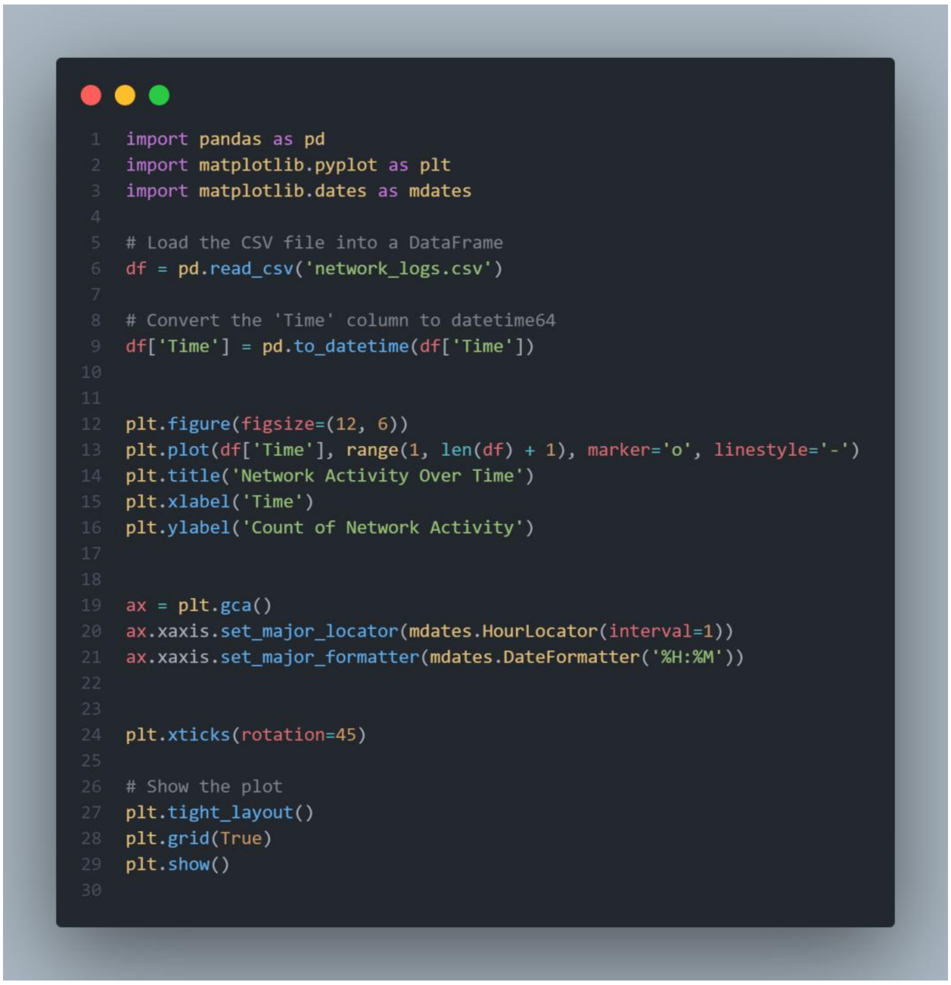
```python
import pandas as pd
import matplotlib.pyplot as plt


df = pd.read_csv('network_logs.csv')


channels = df['Channel']
frequencies = df['Frequency']


plt.figure(figsize=(8, 6))
plt.scatter(channels, frequencies, alpha=0.5, c='b', marker='o')
plt.title('Scatter Plot of Channel vs. Frequency')
plt.xlabel('Channel')
plt.ylabel('Frequency')
plt.grid(True)


plt.show()
```



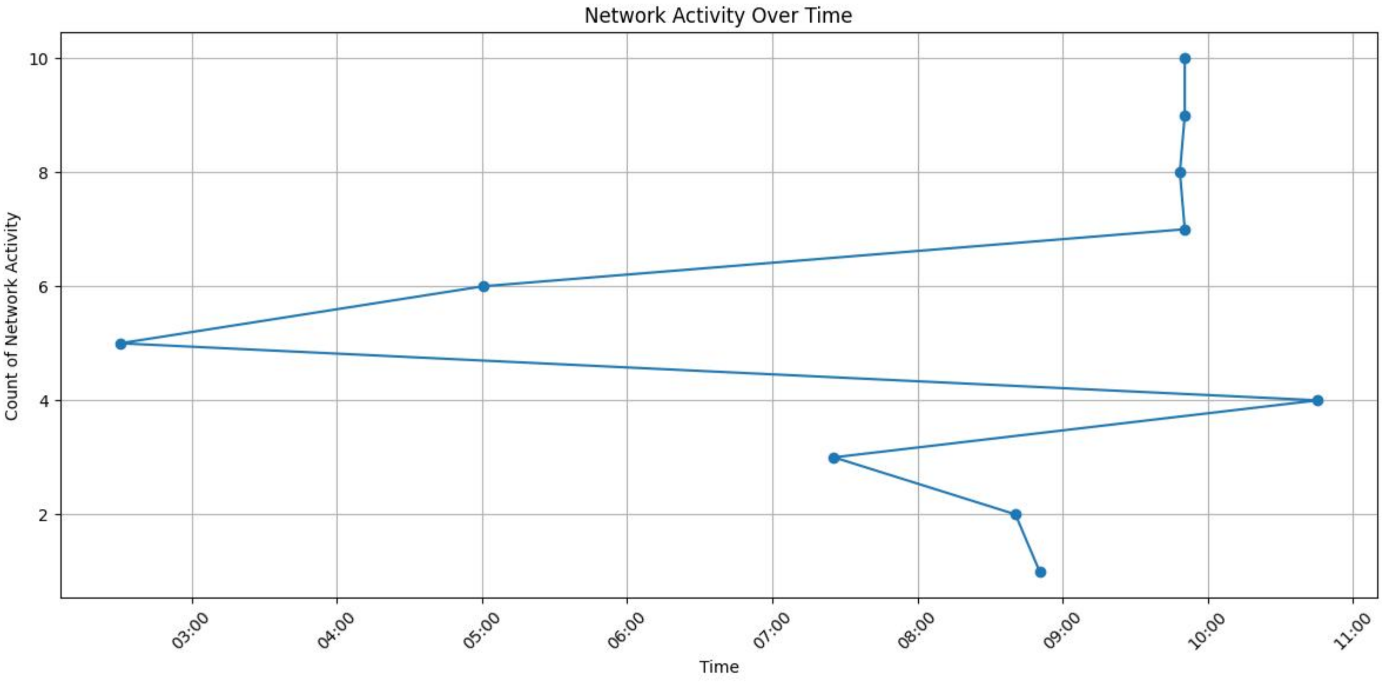


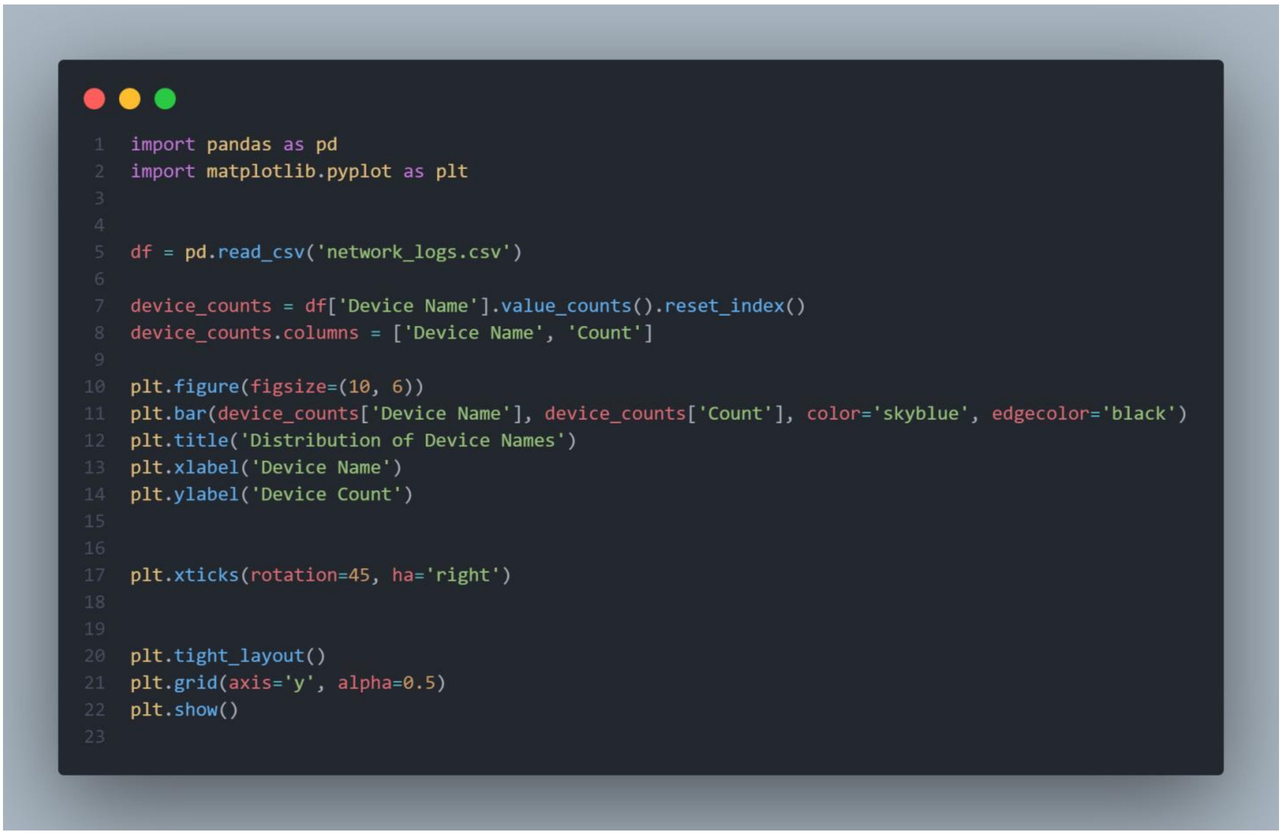
```python
import pandas as pd
import matplotlib.pyplot as plt


df = pd.read_csv('network_logs.csv')

protocol_counts = df['Protocol'].value_counts()

# Create a bar chart
plt.figure(figsize=(10, 6))
protocol_counts.plot(kind='bar', color='skyblue')
plt.title('Protocol Distribution')
plt.xlabel('Protocol')
plt.ylabel('Count')
plt.xticks(rotation=45, ha='right')

# Show the plot
plt.tight_layout()
plt.show()

```



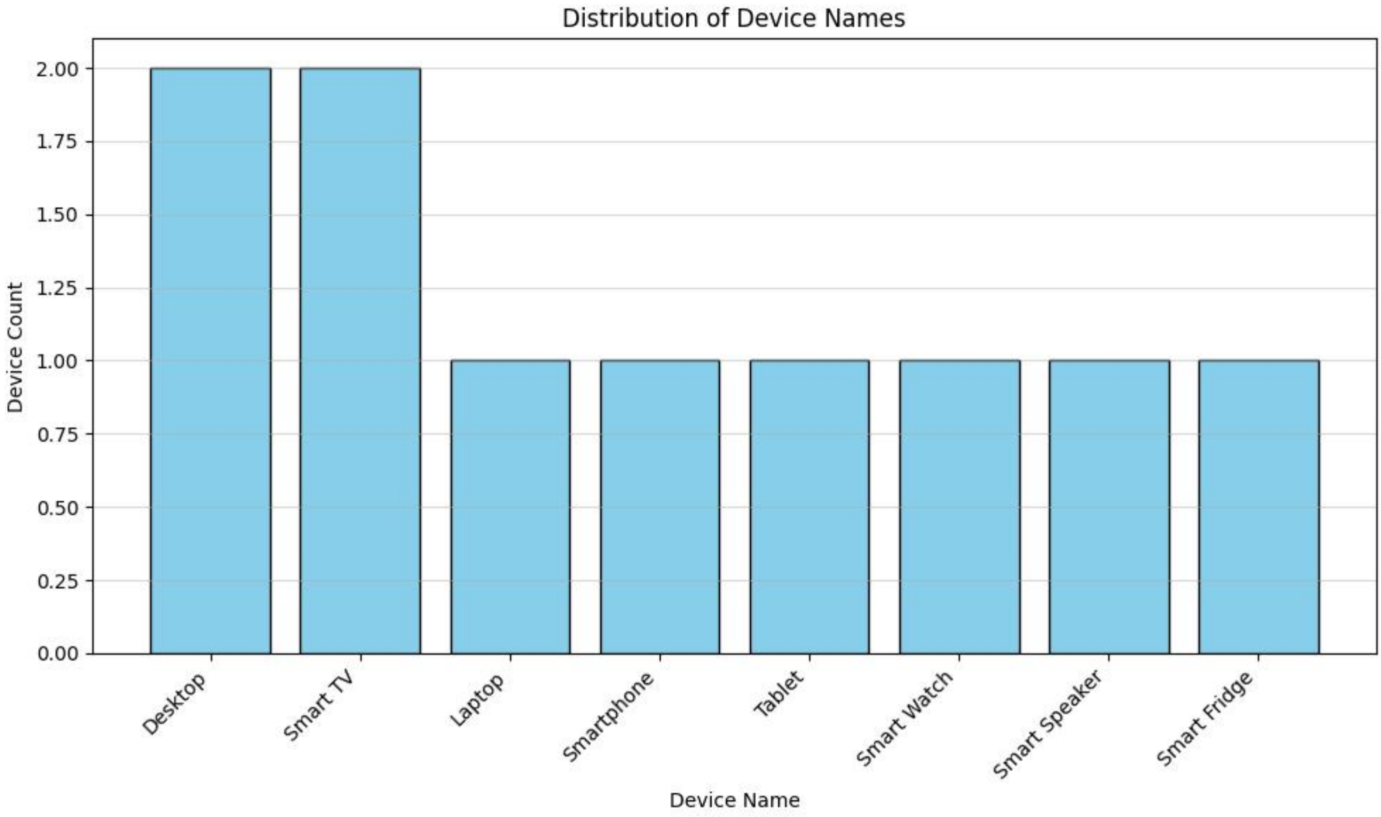


```python
import pandas as pd
import matplotlib.pyplot as plt
import matplotlib.dates as mdates

# Load the CSV file into a DataFrame
df = pd.read_csv('network_logs.csv')

# Convert the 'Time' column to datetime64
df['Time'] = pd.to_datetime(df['Time'])


plt.figure(figsize=(12, 6))
plt.plot(df['Time'], range(1, len(df) + 1), marker='o', linestyle='-')
plt.title('Network Activity Over Time')
plt.xlabel('Time')
plt.ylabel('Count of Network Activity')


ax = plt.gca()
ax.xaxis.set_major_locator(mdates.HourLocator(interval=1))
ax.xaxis.set_major_formatter(mdates.DateFormatter('%H:%M'))


plt.xticks(rotation=45)

# Show the plot
plt.tight_layout()
plt.grid(True)
plt.show()

```





```python
import pandas as pd
import matplotlib.pyplot as plt


df = pd.read_csv('network_logs.csv')

device_counts = df['Device Name'].value_counts().reset_index()
device_counts.columns = ['Device Name', 'Count']

plt.figure(figsize=(10, 6))
plt.bar(device_counts['Device Name'], device_counts['Count'], color='skyblue', edgecolor='black')
plt.title('Distribution of Device Names')
plt.xlabel('Device Name')
plt.ylabel('Device Count')


plt.xticks(rotation=45, ha='right')


plt.tight_layout()
plt.grid(axis='y', alpha=0.5)
plt.show()
```



Conclusion: Thus, we have gained practical knowledge and hands-on experience in configuring wireless routers, capturing network logs, and performing event log analysis.