IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

Vol. 10, Special Issue 2, May 2023

Network Traffic Analysis using Wireshark

Pitamber Chaudhary[1], Vaibhav Kashyap[2], Naresh Sonwal[3], Prasanjeet Panwar[4],Manoj Dadheech[5]

Mrs.Monika Bhatt[6], Mr.Mayank Jain[7]

Student, Computer Science and Engineering, Geetanjali Institute of Technical studies, Udaipur, India[1,2,3,4,5]

Assistant Professor, Computer Science and Engineering, Geetanjali Institute of Technical studies, Udaipur, India[6]

Professor , Computer Science and Engineering, Geetanjali Institute of Technical studies, Udaipur, India[7]

Abstract: Network Traffic Analysis (NTA) refers to the process of examining network traffic to identify patterns, anomalies, and potential security threats. It is a critical aspect of network security and plays a vital role in detecting and preventing cyber-attacks.It involves collecting and analyzing data from various sources, such as network devices, logs, and endpoints, to gain insights into network behavior.It is a primary trace back in network forensics,Packet analysis or we can say Protocol Analysis which describes the process of capturing and interpreting live data as it flows across a network in order to better understand what is happening on the network. This process enables network administrators to identify potential security breaches, data leakage, and other security issues that may jeopardize the confidentiality and integrity of their network.It helps administrators detect suspicious patterns and behaviors, enabling them to respond quickly to potential threats. In summary, NTA is a crucial aspect of network security that aids in detecting, mitigating, and preventing cyber-attacks.

Keywords: Packet sniffing ,Protocol analysis ,Security breaches, Anomaly detection,Cybersecurity

I. INTRODUCTION

In Modern times,Network and the Internet are the backbone of business in terms of sending and receiving ,as it saves time and efforts plus cost.Analysis of the network traffic is one of the most important tools used in network performance analysis and detection of problems such as slow network detect the spammer cause problems in network.It has become an integral part of organizational operations.With increasing reliance on the internet ,cloud services and digital communications tools,networks have become a target for cyber threats .Cyber threats such as hacking , phishing,ransomware and other types of attacks pose significant risks to organization's security , privacy and financial stability.

It has three key components: collection, analysis, and correlation. Collection involves gathering data from various sources, such as network devices, logs, and endpoints. This data may include network packets, flow data, log files, and other types of data. Analysis involves examining the collected data to detect patterns and anomalies. This analysis may involve statistical methods, machine learning, and other techniques Correlation involves linking different data sets to uncover relationships and connections between them.There are different types of techniques for Network Analysis :

1.Packet Capture : It involves capturing network packets and analyzing them to detect potential security threats. Packet capture tools such as Wireshark and tcpdump are commonly used for this purpose.

2. Flow Data Analysis: It involves analyzing NetFlow or sFlow data to detect patterns and anomalies in network traffic.

3. Behavioral Analysis : It involves analyzing network traffic patterns to identify anomalies that may indicate or induce a security threat. Statistical methods and machine learning approaches are used in this.

4.Signature-based Analysis : It involves comparing network network traffic against a database of known signatures of malicious activity.

II. OVERVIEW

Here we are going to take The Packet Capturing approach.We will use Wireshark as a packet sniffer because Wireshark is a widely used open-source network protocol analyzer and packet capture tool. It allows network administrators, security professionals, and developers to analyze and troubleshoot network traffic in real-time. Wireshark provides a comprehensive set of features and capabilities that make it a powerful tool for network analysis.We will try to obtain IP addresses and their respective location from the provided Captured input using Scapy and then visualise it in a table.Before going further let's understand what is Packet capturing.

III. PACKET CAPTURING

It is intercepting a data packet that is crossing a specific point in a data network. Once a packet is captured in real-time, it is stored for a period of time so that it can be analyzed, and then either be downloaded, archived or discarded. Packets are captured and examined to help diagnose and solve network problems such as:

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

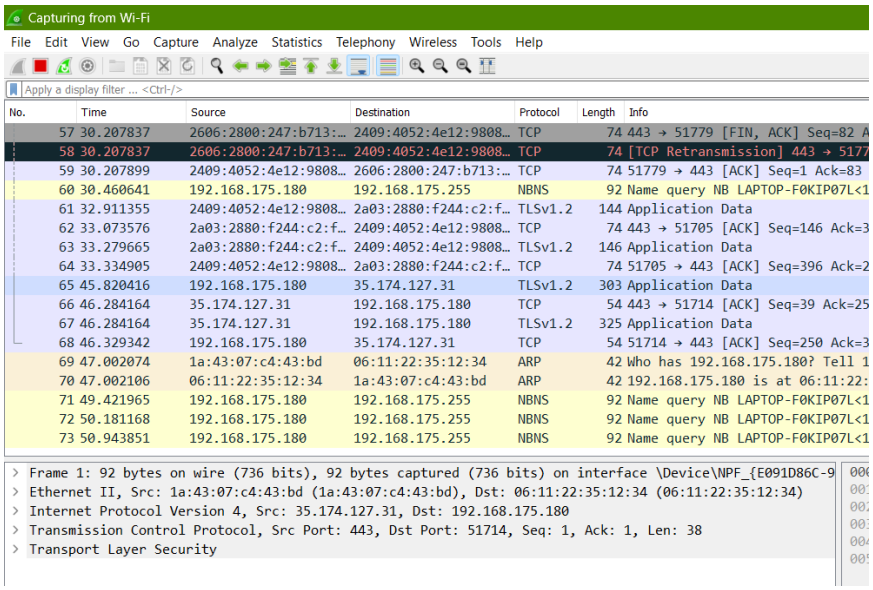
International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

Vol. 10, Special Issue 2, May 2023

- Identifying security threats
- Troubleshooting undesirable network behaviors
- Identifying network congestion
- Identifying data/packet loss
- Forensic network analysis

Packet sniffers can gather almost any type of data. They can record passwords and login information, along with the websites visited by a computer user and what the user viewed while on the site. They can be used by companies to keep track of employee network use and scan incoming traffic for malicious code. In some cases, a packet sniffer can record all traffic on a network
Once you've collected the filtered traffic you can start to look for performance issues. For more targeted analysis you can also filter based on source ports and destination ports to test particular network elements. All of the captured packet information can then be used to troubleshoot network performance issues.



IV. FLOW CHART

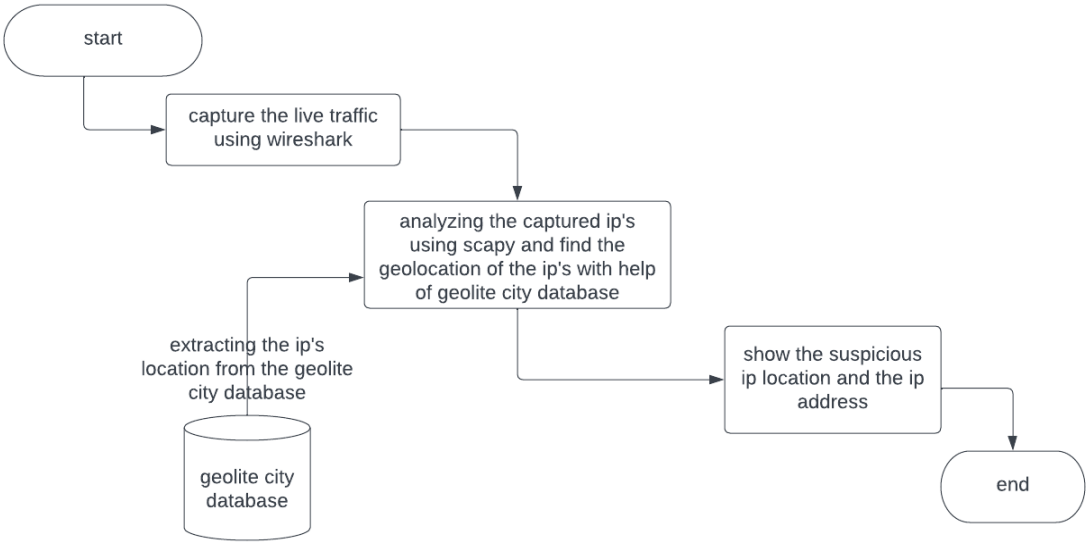


FIG 1: FLOW-CHART OF THE ANALYSIS OF CAPTURED PACKETS

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

Vol. 10, Special Issue 2, May 2023

V. SOFTWARE USED

A. WIRESHARK

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, in May 2006 the project was renamed Wireshark due to trademark issues. Wireshark is cross-platform using pcap to capture packets; it runs on various Unix-like operating systems and on Microsoft Wireshark supports a wide range of network protocols, including TCP/IP, HTTP, DNS, FTP, SSH, and many others. It decodes and analyzes these protocols, providing detailed information about each packet and its corresponding protocol fields. Users can drill down into individual packets to examine specific protocol headers, payload data, and other relevant information. This level of protocol analysis is invaluable for troubleshooting network issues, identifying performance bottlenecks, and detecting security vulnerabilities.

B. PANDAS

It is a popular open-source library in Python that provides high-performance data manipulation and analysis tools. It is widely used by data scientists, analysts, and developers to handle and process structured data efficiently. The name "Pandas" is derived from "panel data" – a term used in econometrics to describe multi-dimensional structured datasets.The main features of Pandas are Data Manipulation,Data Strutures,Data Alignment,Missing Data handling, integrates well with other popular data visualization libraries, such as Matplotlib and It seamlessly integrates with other libraries commonly used in the data science ecosystem, such as NumPy, SciPy, Scikit-learn, and Jupyter Notebook. This integration allows users to leverage the strengths of different libraries and create robust data analysis workflows.

C. GEOLITE DATABASE

GeoLite is a database created by MaxMind, a provider of IP intelligence and geolocation data. The GeoLite database contains geolocation information for IP addresses, allowing users to determine the approximate geographic location of an IP address. It provides insights into the country, region, city, postal code, latitude, and longitude associated with an IP address.It has applications in various domains such as :

a. Website Analytics
b. Fraud Prevention
c. Targeted Advertising
d.Content Localization
e.Network Security

D. SCAPY

It is a powerful Python module that enables the creation, manipulation, and analysis of network packets. It allows network engineers, security professionals, and developers to craft custom network protocols, perform network reconnaissance, simulate network attacks, and conduct network troubleshooting .The main features are Packet manipulation,Packet snoffing and analysis,Network scanning and Network Attack simulation.. With its extensive capabilities and active community, Scapy empowers users to perform advanced network-related tasks with ease and flexibility. [4]

E. STREAMLIT

It is an open-source Python library that simplifies the process of building and deploying interactive web applications for data science and machine learning projects. It enables data scientists and developers to create interactive dashboards, visualizations, and user interfaces with minimal effort and code.It offers a straightforward API that abstracts away the complexities of web development. It provides pre-built components and functions for common tasks such as data visualization, user input widgets, and layout design integrates with popular data visualization libraries such as Matplotlib, Plotly,etc.,and cobines well with machine learning libraries like TensorFlow, PyTorch, and Scikit-learn

VI. RESULT ANALYSIS

A. **Packet Capturing**

IARJSET

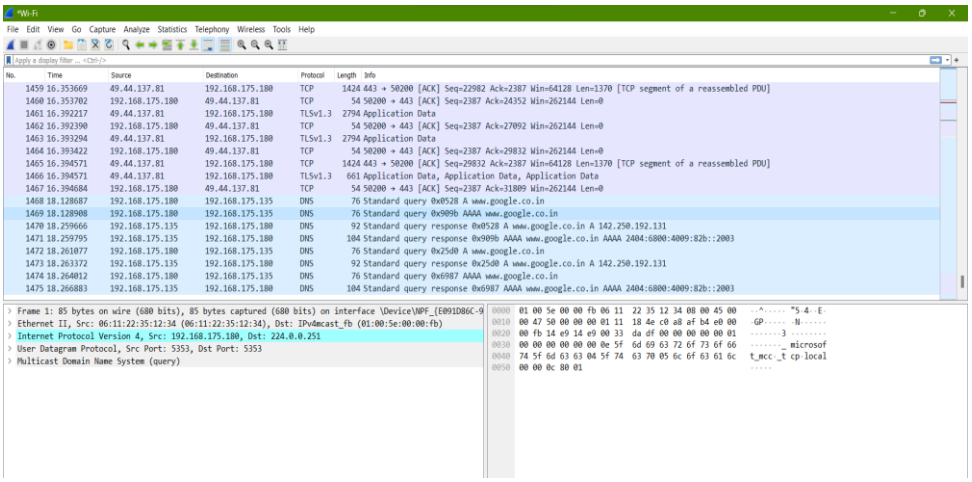
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

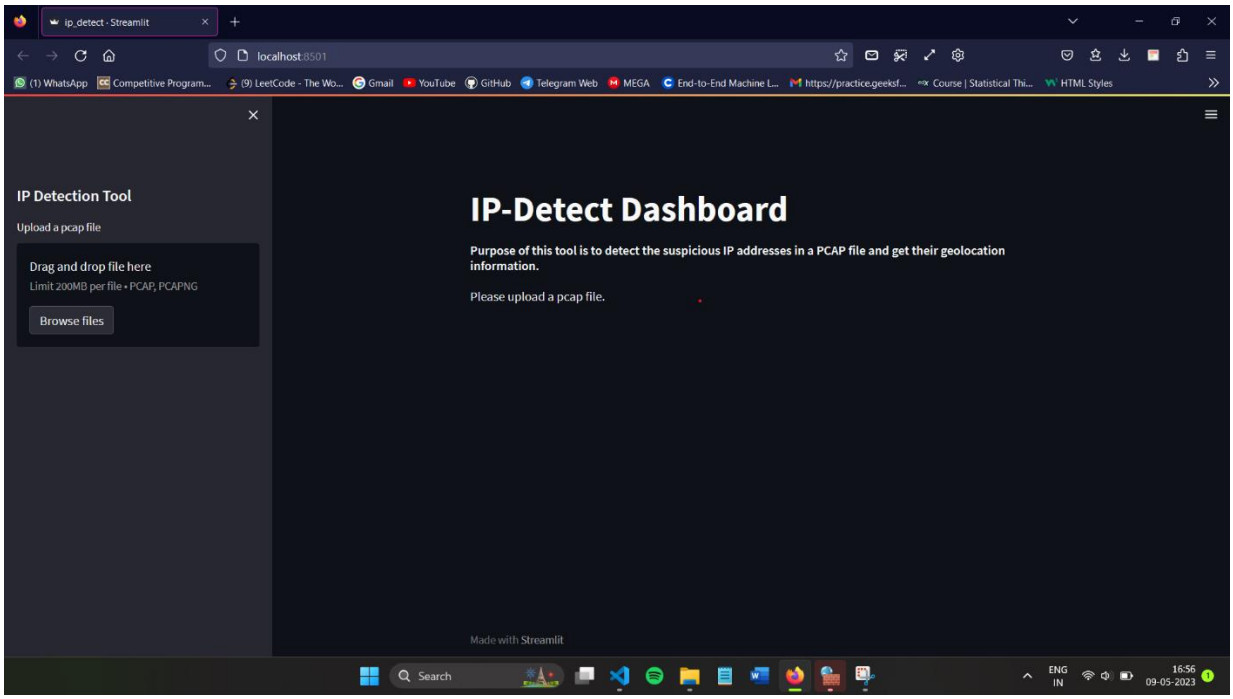
International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

Vol. 10, Special Issue 2, May 2023



B. STARTING ANALYZING TOOL



C. VISUALIZATION OF IP ADDRESSES WITH GEOLOCATIONS

IARJSET

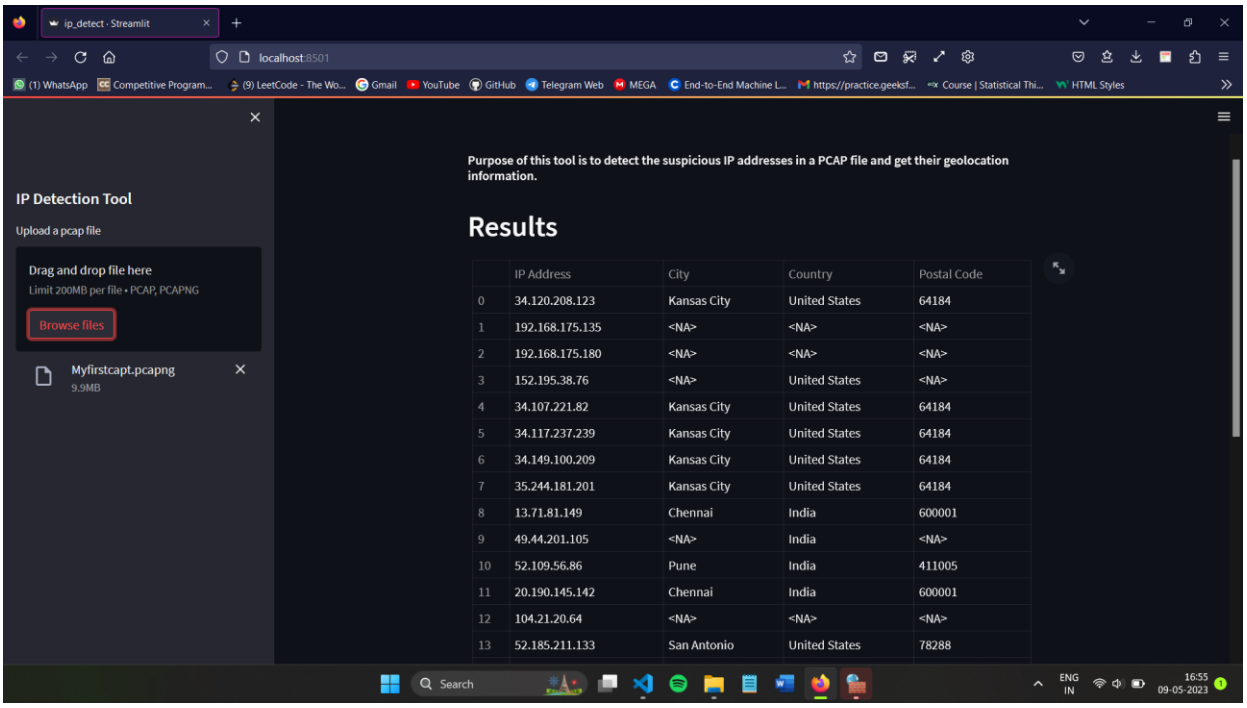
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

Vol. 10, Special Issue 2, May 2023



VII. CONCLUSION

Thus Packet Capturing is useful to analyze tha data during the transmission of network.They are useful for network monitoring,traffic analysis and troubleshooting.By uploading Captured Packets (pcap file) on this tool you will get IP Addresses of given pcap and also the name of City,country and postal code related to them.With IP adderess management ,organizations can track the status and availability of every device in their infrastructure.It is highly useful in preventing Cyber Threats(eg.Active attack) and assaults while ensuring a smooth workflow which enhances the Network Security.

VIII FUTURE SCOPE

The scope of this tool can be further extended by adding features such as detecting Malicious websites ,ransomware protection and to handle Denial of Services (DOS) attacks.A better friendly User interface can be adopted with a streamlined dashboard for better visualizing and tracking data trends.

IX. REFERENCES

[1] www.wireshark.org
[2] BoYu “Based on Network sniffer implement network monitoring Computer Application and System Modeling (ICCASM) 2010 International Conference on Volume: 7,2010,Page(s):V7-1 -v7-3
[3] A Dabir,A Matrawy,”Bottleneck Analysis of Traffic Monitoring Using Wireshark” 4th International conference on Innovations in Information Technology,2007,IEEE Innovations 07,18-20 Nov.2007.Page(s) : 158-162
[4] Ashwani Kumar,Security Attacks in Manet - A Review,2011.
[5] F. Khan, R. Kothari, M. Patel and N. Banoth, "Enhancing Non-Fungible Tokens for the Evolution of Blockchain Technology," 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2022, pp. 1148-1153, doi: https://doi.org/10.1109/ICSCDS53736.2022.9760849
[6]] D.Madhavi,TCP Session Hijacking Implementation by Stealing Cook-ies,Vol. 2, Issue 11, 2015
[7] Ankita Gupta, Kavita, Kirandeep Kaur,Vulnerability Assessment and
[8] Penetration Testing,International Journal of Engineering Trends andTechnology- Volume4Issue3- 2013.
[9] Natarajan Meghanathan, Sumanth Reddy Allam and Loretta A.
[10] D. Kothari, M. Patel and A. K. Sharma, "Implementation of Grey Scale Normalization in Machine Learning & Artificial Intelligence for Bioinformatics using Convolutional Neural Networks," 2021 6th International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2021, pp. 1071-1074, https://doi.org/10.1109/ICICT50816.2021.9358549.
[11] Moore,TOOLS AND TECHNIQUES FOR NETWORK FORENSICS,IJNSA, Vol .1, No.1,April 2009 .