SEPARATION OF TRAFFIC BASED ON APPLICATION LAYER PROTOCOLS AND ASSOCIATED STATISTICS

A MINI PROJECT REPORT

SUBMITTED BY

MK JAYANTH SHANMUGAM & MANAV ANANTHAKUMAR

In partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE & ENGINEERING

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
A Constituent Institution of Manipal University

Department of Computer Science & Engineering

NOVEMBER 2021

Department of Computer Science & Engineering

BONAFIDE CERTIFICATE

Certified that this project report "Separation of Traffic Based on Application Layer Protocols and Associated Statistics" is the bonafide work of MK Jayanth Shanmugam & Manav Ananthakumar who carried out the mini project work under my supervision.

Submitted to the Viva voce Examination held on

30th November 2021

EXAMINER 1 EXAMINER 2

ABSTRACT

Packet analysis is a primary traceback technique in network forensics, which, providing that the packet details captured are sufficiently detailed, can play back even the entire network traffic for a particular point in time. This can be used to find traces of nefarious online behavior, data breaches, unauthorized website access, malware infection, and intrusion attempts, and to reconstruct image files, documents, email attachments, etc. sent over the network. This project focuses on the very basics of packet analysis by capturing the network data through Wireshark, filtering out the packets which belong to application layer protocols and displaying statistics related to them such as the packet count of each protocol and the average packet length.

Pandas is a python package used for data analysis. Wireshark is a cross-platform tool capable of capturing vast amounts of data. Using Wireshark, we made a csv file to perform analysis. Using pandas, doing packet analysis is simple and functions for basic operations are inbuilt. We created two functions, the first one to print the packet count of application layer protocols in the traffic. The second function to find the average packet size of each application layer protocol in the traffic and print it.

ACKNOWLEDGEMENT

We would like to express our special thanks of gratitude to our Computer Networks teacher Dr. Arun Kumar for providing us the resources and knowledge required to complete this project. Through this project we were able to gain a lot of practical knowledge which according to us is a very crucial part in our career.

We would also like to thank our friends who supported us throughout the way in completing this project.

MK Jayanth Shanmugam-190905276

Manav Ananthakumar-190905199

CSE SECTION A

TABLE OF CONTENTS

1. Cover Page & Title Page ----------1

2. Bonafide Certificate ----------2

3. Abstract ----------3

4. Acknowledgement ----------4

5. Introduction ----------6

6. Method Used ----------7

7. Results ----------8

8. References ----------9

Introduction

The Application Layer is the topmost layer in the Open System Interconnection (OSI) model. This layer provides several ways for manipulating the data (information) which actually enables any type of user to access network with ease. This layer also makes a request to its bottom layer, which is transport layer for receiving various types of information from it. The Application Layer interface directly interacts with application and provides common web application services. This layer is basically the highest level of open system, which provides services directly for application processes.

Services provided by the Application Layer

1. **Mail Services:** This layer provides the basis for E-mail forwarding and storage. Protocols used – HTTP, SMTP, POP3, IMAP, HTTPS
2. **Directory Services:** This layer provides access for global information about various services. Protocols – DHCP, DNS.
3. **File Transfer, Access and Management (FTAM):** It is a standard mechanism to access files and manages it. Users can access files in a remote computer and manage it. They can also retrieve files from a remote computer. Protocols – FTP, FTP-DATA.
4. **Network virtual terminal:** Allows the user to log onto a remote host. The user's computer talks to the software terminal which in turn talks the host. Protocols – Telnet

Method Used

- The desktop application *WireShark* was used to capture the incoming and outgoing traffic from a laptop connected to the college Wi-Fi. The traffic captured was exported as a CSV file.
- A Python script was written to analyze the traffic and separate the packets based on the various application layer protocols mentioned above in the introduction.
- The *Pandas* library was used to filter out the packets that belong to one of the application layer protocols mentioned in the introduction above.
- The total number of packets for each application layer protocol and the average packet length of a packet was calculated using the various functions in the library.
- The total number of packets and the average packet length was put into an excel file and a histogram was made for the analyzed data.

Results

The Highest number of packets was found to be those that belonged to TLSv1.3/HTTPS.

Due to large volume of net surfing.

Protocol	Packet Count
DHCP	2
DNS	1440
FTP	47
FTP-DATA	320
HTTP	11
OCSP	166
TLSv1.2	2113
TLSv1.3	7261

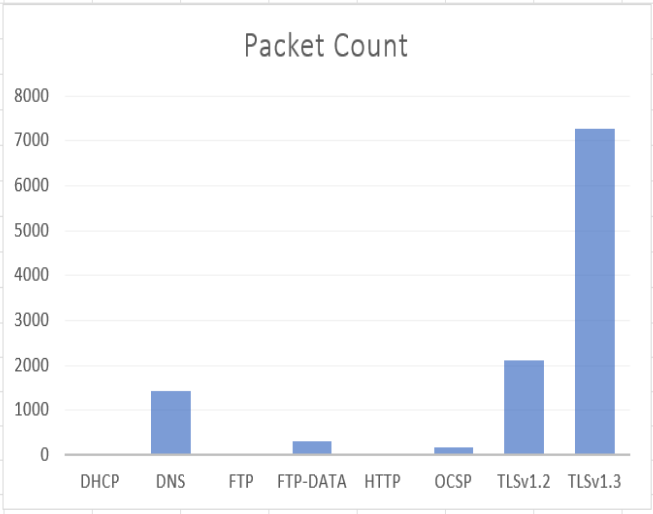

Fig 1.1: Histogram of the packet count of each application layer protocol in traffic.

Highest average packet length was for FTP-DATA as large amounts of data was transferred.

Protocol	Average Packet Length
DHCP	350
DNS	183.8520833
FTP	82.10638298
FTP-DATA	1392.059375
HTTP	340.4545455
OCSP	668.7108434
TLSv1.2	744.6209181
TLSv1.3	951.6682275

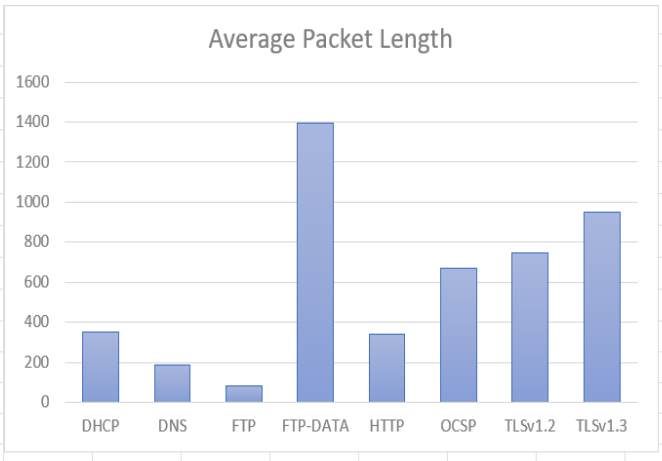

Fig 1.2: Histogram of the average packet length of each application layer protocol in traffic.

References

- *https://www.studytonight.com/computer-networks/osi-model-application-layer*
- *https://www.python4networkengineers.com/posts/wireshark/analyzing_wireshark_data_with_pandas/*