PCAP FILE ANALYZER FOR NETWORK FORENSIC

WAN MUHAMMAD KHAIRUDDIN BIN WAN AB KARIM

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN

JUDUL: PCAP FILE ANALYZER FOR NETWORK FORENSIC

SESI PENGAJIAN: 2022 / 2023

Saya: WAN MUHAMMAD KHAIRUDDIN BIN WAN AB KARIM

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan unituk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. * Sila tandakan (✓)

___________ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

___________ TERHAD ✓(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)

✓__________ TIDAK TERHAD

(TANDATANGAN PELAJAR)

Alamat tetap:

36-03-03 Sri Tioman 1, Jalan Tumbuhan,
Taman Melati 53100 Kuala Lumpur

(TANDATANGAN PENYELIA)

Dr Nur Fadzilah Binti Othman
Nama Penyelia

PCAP FILE ANALYZER FOR NETWORK FORENSIC

WAN MUHAMMAD KHAIRUDDIN BIN WAN AB KARIM

This report is submitted in partial fulfillment of the requirements for the Bachelor of Computer Science (Computer Security) with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DECLARATION

I hereby declare that this project report entitled

PCAP FILE ANALYZER FOR NETWORK FORENSIC

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : ______________________________ Date : 20/9/2023

(WAN MUHAMMAD KHAIRUDDIN BIN WAN AB KARIM)

I hereby declare that I have read this project report and found this project report is sufficient in term of the scope and quality for the award of Bachelor of Computer Science (Computer Security) with Honours.

SUPERVISOR : ______________________________ Date : 25/9/2023

(DR NUR FADZILAH BINTI OTHMAN)

DEDICATION

This research study is dedicated to the unwavering love and support of my parents, who have been the cornerstone of my academic journey. Their sacrifices and encouragement have profoundly shaped my character and contributed to my growth as an individual. This achievement stands as a testament to their enduring dedication and the values they have instilled in me.

I extend my deepest gratitude to my esteemed supervisor, Dr. Nur Fadzilah Binti Othman, for their invaluable mentorship and guidance. Their expertise, unwavering passion for knowledge, and unwavering belief in my potential have consistently inspired me to strive for excellence and reach new heights.

Lastly, I dedicate this research study to myself. It symbolizes my unwavering determination, resilience, and commitment to personal and academic development. It serves as a constant reminder of my ability to overcome challenges and achieve my aspirations. I take immense pride in the dedication and effort I have invested.

To my parents, my supervisor, and myself, I express heartfelt appreciation for your indispensable roles in this research study. Your unwavering support, invaluable guidance, and unshakeable belief in my abilities have been the driving force behind my accomplishments.

ACKNOWLEDGEMENT

I am profoundly grateful to Universiti Teknikal Malaysia Melaka (UTeM) for granting us, undergraduate students from the Faculty of Information and Communication Technology (FICTS), an invaluable opportunity to embark on our final year project expedition.

Furthermore, I wish to extend my deepest appreciation to my supervisor, Dr. Nur Fadzilah Binti Othman, for their unwavering support, invaluable guidance, and expert mentorship throughout the course of this project. Their extensive knowledge, constructive feedback, and unwavering commitment to excellence have played an integral role in shaping the trajectory and caliber of this research endeavor. I am truly indebted to their continuous encouragement and steadfast belief in my abilities.

Additionally, I am thankful to my fellow classmates and friends for their unwavering support, encouragement, and engaging discussions that have greatly enriched my comprehension of the subject matter. Their camaraderie and shared experiences have made this research expedition more fulfilling and etched indelible memories.

Lastly, I wish to express profound gratitude to my parents, Wan Ab Karim bin Wan Mohd Ghazali and Siti Hasni Binti Taslim, for their unwavering love, unwavering encouragement, and unwavering understanding throughout my academic pursuit. Their unwavering faith in my capabilities and the sacrifices they have made have been the propelling force behind my accomplishments.

ABSTRACT

PCAP file is a file that is commonly used by network forensic analyst to preserve network connection and to do inclvestigation on network. PCAP file used to capture and store network traffic that contains network packets and its' information about it. In PCAP file, there is so many information can be extracted such as source and destination IP address, packet's payload and other types of metadata. Many tools can be used to perform analysis on PCAP file such as Tshark, wireshark or Network Miner. In previous research, a PCAPFunnel tool is developed to provide a visualization to PCAP file. This tool uses Tshark as its backend processing to extract data from PCAP file and use the front end framework to visualize extracted data. This tool mainly focus on visualization of data. In this project, it extend the capability of a single network forensic tool from providing just a visualization of data to another multiple feature such as deep packet inspection, file extraction, and strings extraction.

ABSTRAK

Fail PCAP ialah fail yang biasa digunakan oleh penganalisis forensik rangkaian untuk mengekalkan sambungan rangkaian dan untuk melakukan penyiasatan pada rangkaian. Fail PCAP digunakan untuk menangkap dan menyimpan trafik rangkaian yang mengandungi paket rangkaian dan maklumat mengenainya. Dalam fail PCAP, terdapat begitu banyak maklumat yang boleh diekstrak seperti alamat IP sumber dan destinasi, muatan paket dan jenis metadata lain. Banyak alatan boleh digunakan untuk melakukan analisis pada fail PCAP seperti Tshark, wireshark atau Network Miner. Dalam penyelidikan terdahulu, alat PCAPFunnel dibangunkan untuk menyediakan visualisasi kepada fail PCAP. Alat ini menggunakan Tshark sebagai pemprosesannya untuk mengekstrak data daripada fail PCAP dan menggunakan 'front end framework' untuk menggambarkan data yang diekstrak. Alat ini dibangunkan dengan tujuan terutamanya pada visualisasi data. Dalam projek ini, alatan yang akan di bangunkan, memanjangkan keupayaan alat forensik rangkaian daripada menyediakan hanya visualisasi data kepada ciri-ciri lain seperti pemeriksaan paket dalam, pengekstrakan fail dan pengekstrakan rentetan.

TABLE OF CONTENTS

DECLARATION i
DEDICATION ii
ACKNOWLEDGEMENT iii
ABSTRACT iv
CHAPTER 1: INTRODUCTION 1
1.1 Introduction 1
1.2 Problem Statement 2
1.3 Project Question 2
1.4 Project Objective 3
1.5 Project Scope 3
1.6 Project Contribution 3
1.7 Thesis Organization 4
1.7.1 Chapter 1: Introduction 4
1.7.2 Chapter 2: Literature review 4
1.7.3 Chapter 3: Methodology 4
1.7.4 Chapter 4: Design 4
1.7.5 Chapter 5: Implementation 4
1.7.6 Chapter 6: Testing 4
1.7.7 Chapter 7: Conclusion 4
1.8 Conclusion 5
CHAPTER 2: LITERATURE REVIEW 6
2.1 Introduction 6
2.2 Network Forensic 6
2.3 PCAP file 7
2.4 Methodology in network forensic analysis 8
2.4.1 Protocol Parsing and Analysis 8
2.4.2 Deep Packet Inspection 8
2.5 Other tools in network forensic (Related work) 10
2.5.1 Wireshark 10
2.5.2 Tshark 12
2.5.3 PCAPFunnel 13

2.5.4 Network Miner ... 14

2.6 Features and characteristic ... 16

2.6.1 Visualization of Data ... 16

2.6.2 Detail Packet Inspection ... 17

2.6.3 File Extraction ... 17

2.6.4 Strings Extraction ... 18

2.7 Critical Review ... 19

2.8 Proposed Solution ... 19

2.9 Conclusion ... 19

CHAPTER 3: PROJECT METHODOLOGY ... 20

3.1 Introduction ... 20

3.2 Methodology ... 20

3.3 Project Milestone ... 21

3.4 Gantt Chart ... 27

3.5 Conclusion ... 28

CHAPTER 4: DESIGN ... 29

4.1 Introduction ... 29

4.2 Requirement Identification ... 29

4.3 Requirement Analysis ... 31

4.3.1 Data Requirement ... 31

4.3.2 Functional Requirement ... 31

4.3.3 Non-functional Requirement ... 32

4.3.4 Other Requirements ... 32

4.3.4.1 Software Requirements ... 32

4.4 High-level Design ... 34

4.4.1 Software Design ... 34

4.4.2 API Design ... 35

4.4.2.1 Protocol Parser ... 36

4.4.2.2 Strings Extraction ... 39

4.4.2.3 JSON Output ... 40

4.4.3 User Interface Design ... 42

4.4.3.1 Main Interface ... 43

4.4.3.2 Upload ... 46

4.4.3.3 System Flow ... 47

4.5 Conclusion ... 47

CHAPTER 5: IMPLEMENTATION ... 48

5.1 Introduction ... 48

5.2 Software development environment setup 48
5.3 API Development 49
5.3.1 Configuration Setup 50
5.3.2 Upload 51
5.3.3 Dashboard 52
5.3.4 Projects 53
5.3.5 Current Project 53
5.3.6 Protocols 53
5.3.7 Hosts 54
5.3.8 Packets 55
5.4 Protocol Parsers 57
5.4.1 HTTP Parser 57
5.4.2 FTP Parser 61
5.4.3 Telnet Parser 64
5.5 Other Feature Implementations 65
5.5.1 Strings Extraction 65
5.5.2 File Extraction 68
5.6 User interface and front-end 69
5.6.1 Upload page 69
5.6.2 Dashboard Page 71
5.6.3 Connections Page 73
5.6.4 Protocols Page 75
5.6.5 Strings Page 79
5.6.6 Files Page 80
5.7 Version Control Management 81
5.8 Conclusion 81
CHAPTER 6: TESTING 82
6.1 Introduction 82
6.2 Test Plan 82
6.2.1 Test Schedule 82
6.2.2 Test Strategy 82
6.3 Test Design 82
6.3.1 Test Cases 82
6.4 Test Result & Analysis 85
6.4.1 Upload Feature Testing 85
6.4.2 Connections Feature Testing 86
6.4.3 Protocols Feature Testing 87

6.4.4 Find Strings Feature Testing 89
6.4.5 File Extraction Feature Testing 91
6.5 Conclusion 93
CHAPTER 7: CONCLUSION........ 94
7.1 Introduction 94
7.2 Project Summarization 94
7.3 Project Contribution 95
7.4 Limitation 95
7.5 Future Works 96
7.6 Conclusion 96
Reference 102

LIST OF FIGURES

Figure 2.1 Different between stateful and deep packet inspection 9
Figure 2.2 Wireshark 10
Figure 2.3 Wireshark filter 11
Figure 2.4 Tshark CLI tool 12
Figure 2.5 Tshark filter feature 13
Figure 2.6 PCAPFunnel 14
Figure 2.7 Network Miner 15
Figure 2.7 File extraction feature on Network Miner 16
Figure 4.1 Software activity diagram 35
Figure 4.2 Tool's API flowchart 36
Figure 4.3 Flowchart of protocol parser 37
Figure 4.4 Flowchart of parsing request and response 38
Figure 4.5 Flowchart of string extraction 40
Figure 4.6 JSON structure for every network protocol 41
Figure 4.7 JSON structure for matched strings 42
Figure 4.8 Main interface 43
Figure 4.9 Connection tab interface 44
Figure 4.10 Protocols tab interface 44
Figure 4.11 View more detail packet information 45
Figure 4.12 Extract strings tab interface 45
Figure 4.13 Files tab interface 46
Figure 4.14 Upload interface 46
Figure 4.15 System flowchart 47
Figure 5.1 Upload page 70
Figure 5.2 Go to dashboard button appear 70
Figure 5.3 Dashboard page 72
Figure 5.4 Connections page 73
Figure 5.5 Protocol page 75
Figure 5.6 Connections show in connections column 76
Figure 5.7 All packets shown in packets column 77
Figure 5.8 Detail packet inspection 78
Figure 5.9 Strings page 79
Figure 1.10 Files page 80
Figure 6.1 Uploading file to application 85
Figure 6.2 Dashboard appears 85
Figure 6.3 Output files created in local folder 86
Figure 6.4 Upload simple file 86
Figure 6.5 Visiting the connections page 87
Figure 6.6 rearrange the order by dragging the icon 87
Figure 6.7 Upload sample file 88
Figure 6.8 Visit protocols page 88
Figure 6.9 Protocol button clicked 89
Figure 6.10 Choose any connection 89
Figure 6.11 Display detail packet 89

Figure 6.13 Alert box appear after submit the regular expression 91
Figure 6.14 The output appears.. 91
Figure 6.15 A lot of connection from PCAP file.. 92
Figure 6.16 List of extracted files 92
Figure 4.8 The image can be view by clicking on it 93

LIST OF TABLES

Table 1.1 List of problem statements 2
Table 1.2 List of project questions 2
Table 1.3 List of project objectives 3
Table 1.4 List of Project contributions 3
Table 2.1 Summarize of features 19
Table 3.1 Milestone for PSM1 22
Table 3.2 Milestone for PSM2 24
Table 3.3 Gantt chart for PSM 1 27
Table 3.4 Gantt chart for PSM 2 27
Table 6.1 Test case 01 – upload feature 82
Table 6.2 Test case 02 – connection feature 83
Table 6.3 Test case 03 – protocol feature 83
Table 6.4 Test case 04 – strings extraction feature 84
Table 6.5 Test case 05 – file feature 84

CHAPTER 1: INTRODUCTION

1.1 Introduction

In this current era, everything has turned digital. From businesses to normal people, everyone starts to use the internet to communicate, shop, entertainment, and learning. People also start to subscribe to internet connection. According to the Department of Statistics in the Ministry of Economy Malaysia, More and more households are now using technology. This includes computers (88.3%), the Internet (95.5%), mobile phones (99.6%), radios (98.9%), TV (99.0%), pay TV (83.2%), and fixed-line phones (31.3%). Now the internet has become essential in daily life. As the usage of technology and internet increases, cybercrime also increases. Cybercrime like phishing, personal data breach, extortion or ransomware are a few of the most popular attacks based on the statistic from Statista.

While cybercrimes are rapidly growing, the efforts to take down the operation also increase. The blue team and digital forensics are two fields that help in protecting assets from being attacked. Digital forensics helps track down the threat author and make sure they got caught and brought to justice. In the digital world, every action is recorded and can be tracked especially anything that happens in a network because connection in network can be recorded, so any malicious event can be thoroughly analyzed by the expert like digital forensic analyst. Digital forensic analyst is the person who responsible searching for evidence of the crime. They will use tools to analyze artifacts that they got from crime scenes and extract any useful information. Having an efficient and simple tool is a big help to the analyst since it will help them extract information or evidence effectively in a big network. Today, these tools are available in the market. But these tools are different from each other. Different tools offer different functionalities. To use these functionalities, the user might want to open multiple tools at same time. So, a tool that combined all features together can make network analysis easier.

1.2 Problem Statement

In network forensics, the recorded network connection is the most important artifact because it contains so much information and evidence. Network forensic analyst will analyze a file that is called a packet capture or PCAP file. This file can be analyzed manually using a tool such as Wireshark. Doing a manual network analysis on a PCAP file using tools like Wireshark can consume a lot of time searching and finding evidence because analyst needs to figure out the scenario of the attack first before they can know what other things to look for. There are also several weaknesses using existing tools to do network forensic such as:

Table 1.1 List of problem statements

PS	**Problem Statement**
PS1	Existing tools have separate feature for different tools
PS2	User needs to open multiple tools to use different feature
PS3	Existing tool is quite complicated to use

1.3 Project Question

Project questions are usually derived from problem statements. It is important to know the questions to solve the problem statement that we had listed.

Table 1.2 List of project questions

PQ	**Project Question**
PQ1	What is the feature offers by different PCAP analyzer tools?
PQ2	How to create tools where user does not have to open multiple tools at a time?
PQ3	How to make tool simple to use?

1.4 Project Objective

To provide the solutions for the problems and answer the questions that are raised, we come up with objectives to achieve.

Table 1.3 List of project objectives

PO	**Project Objective**
PO1	To identify features for PCAP file analyzer
PO2	To develop a PCAP analyzer tool that have multiple feature
PO3	To test PCAP analyzer tool to make sure it is easy to use

1.5 Project Scope

The project scope will be conducted based on the project objectives to ensure the correct and organized flow of the project. The scope of the project include:

1. This application is meant to be used in a network forensic investigation to analyze packet capture files. It cannot analyze live traffic.
2. This application can only analyze PCAP files. The project does not cover Netflows file.
3. The application will be a web based where the user will run the tools in a form of web locally using docker.
4. The application can perform accordingly if the PCAP file is small.

1.6 Project Contribution

After the project is finished, we expect the project will contribute something to the network forensic. The contribution of our project is as follow:

Table 1.4 List of Project contributions

PC	**Project Contribution**
PC1	Provide an application that has the capability to make network forensic analyst look for evidence efficiently
PC2	Provide a Network Forensic Analysis Tool (NFAT) to network forensic analyst to analyze PCAP file
PC3	To provide a way of organizing information

1.7 Thesis Organization

1.7.1 Chapter 1: Introduction

This chapter introduces and explains the background of the project. It explains the problem statement, objective, project scope and contribution of the project. It also explains the issues that arise that lead to the development of the project.

1.7.2 Chapter 2: Literature review

This chapter describes more about projects which are supported by details from past projects and research papers.

1.7.3 Chapter 3: Methodology

This chapter outlines the methods and procedures used to conduct the study. It provides a detailed description of how the research was designed, the data collection process, and the analysis techniques employed.

1.7.4 Chapter 4: Design

The design chapter focuses on the overall design or framework of the study. It outlines the structure, organization, and plan for conducting the project. The design chapter provides a blueprint for the research process and helps readers understand how the study was organized and executed.

1.7.5 Chapter 5: Implementation

The implementation chapter focuses on the practical execution of the project and details the steps taken to develop and deploy the intended solution or product. This chapter provides an account of how the project was carried out, including the activities, resources, and processes involved in the implementation phase.

1.7.6 Chapter 6: Testing

The testing chapter focuses on the activities and processes related to testing the software or product being developed. It outlines the strategies, methodologies, and techniques employed to ensure the quality, reliability, and functionality of the solution. The testing chapter provides a comprehensive account of the testing efforts carried out during the development lifecycle.

1.7.7 Chapter 7: Conclusion

The conclusion chapter serves as the final section of the project report or thesis. It summarizes the key findings, achievements, and implications of the project. The conclusion chapter provides closure to the project by summarizing the overall outcomes and offering insights and recommendations for future work.

1.8 Conclusion

As a conclusion, this project is design to introduce new network forensic tools that can help network forensic analyst to understand the incident and to obtain the evidence from a PCAP file. These tools also will be an improvement from previous tools that will be covered in the next chapter.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

In this chapter, we are going through several research papers that are related to network forensics, discussing, and understanding the process involved in network forensic and the tools that are used in gathering evidence. This literature review is the part where the ideas that are useful to the project are considered.

2.2 Network Forensic

Network forensics is a subfield of digital forensics that involves the collection, analysis, and interpretation of network traffic data to investigate and determine the cause of security incidents or network performance issues. Network forensics includes a process of capturing, recording and analysis of network traffic to discover malicious activity in a network (Liu, C., 2015). Network forensics is a process of detecting the intrusion pattern and focusing on attacker activity. It is a vital tool for identifying and responding to security incidents, as it provides valuable information about how an attacker gained access to a network, what data they accessed, and how they exfiltrated that data.

The process of network forensics typically involves the practice of gathering data that travels over a network and attempting to interpret it in some way. Reconstructive traffic analysis is the foundation of this approach. It could be utilized for forensic investigation to read and examine the contents of raw PCAP Internet data for a specific network session (Manesh, T. et al, 2011).

The analysis of network traffic data can provide valuable information about the behavior of individual users and groups of users on the network. This information can be used to identify policy violations, such as unauthorized use of company resources, or to detect insider threats, such as employees who are stealing company data.

Network forensics is a critical component of modern cybersecurity and is used by organizations of all sizes and types to protect their networks and data. By leveraging network forensics techniques, organizations can detect and respond to security incidents quickly, minimize the impact of security breaches, and improve overall network performance and security.

2.3 PCAP file

A PCAP file is a container for packets captured on a computer network, such as a WiFi or Ethernet network. A timestamp identifying the moment the packet was collected is attached to each packet in a PCAP file. The abbreviation PCAP stands for Packet CAPture. The terms capture file, trace file, packet trace, packet dump, dumpfile, and pcap savefile are also frequently used. Around 1987, Van Jacobson, Craig Leres, and Steven McCanne were working at the Lawrence Berkeley Laboratory on tcpdump and libpcap when they developed the PCAP file format. (Netresec, 2022)

All the ethernet packets that were recorded from the ethernet card are included in this file. This can be done utilizing our software's capture feature or other programs like "Wireshark" that support the PCAP format. This file is subjected to the analysis procedure (Manesh, T. et al, 2011).

There are various versions of PCAP files, each with its own capabilities and applications. For instance, WinPcap is a format tailored for Windows devices, functioning as a portable packet capture library. Libpcap, an open-source C++ library, is utilized by Mac OS and Linux devices for packet capture and filtering, often employed by packet sniffing tools. Npcap, on the other hand, is a packet sniffing library known for its fast and secure functionalities, specifically designed for Windows devices. Additionally, PCAPng allows users to perform loopback packet capture injection and sniff loopback packets (Solarwinds).

The PCAP file can be used by a network forensic analyst to determine and investigate crimes that happen in a network because it can provide valuable information that gives the analyst insight into any threats, crimes, and attacks happening in the network. The analyst can find and collect evidence found in the PCAP file, such as the IP address of the threat actor, the data exfiltrated from the network, or even an exploit used on the network. It can also be used to analyze the behavior of malware inside the network when security analysts find new malware not previously analyzed. Other than that, as a network administrator, PCAP files can be used to monitor performance and analyze any traffic issues.

In summary, PCAP files are binary data files containing a log of network traffic captured by network monitoring and analysis tools. They provide valuable insights into network behavior and can be used for network troubleshooting, analysis, and security purposes.

2.4 Methodology in network forensic analysis

This part discusses a few techniques that are used in network forensic analysis. This helps create an overview of what are the things that are often looked at during network forensic analysis and how the data are found.

2.4.1 Protocol Parsing and Analysis

Researchers often conduct protocol analysis manually using a combination of tools. They start by running tcpdump to capture network traffic and then use strings to extract text from the captured data. By applying grep, which is a tool that is installed in Unix machine, they can search for specific words or phrases within the extracted strings. This approach can yield valuable information about the network's web traffic. For example, identifying the string “get” can provide insights into web requests. Differentiating between protocols requires further analysis. For instance, a session containing the string “quit” could indicate an FTP control session, POP3 session, or NNTP session. On the other hand, the presence of “privmsg” suggests an Internet Relay Chat (IRC) session. Examining a TCP connection on port 23 with Telnet interpret-as-command sequences (IACs) likely indicates Telnet usage. However, a session on the same port featuring the string “YMSG” and "c0 80" record separators is more likely associated with Yahoo Messenger (Shearin, S. et al, 2002).

In summary, analysts employ manual protocol analysis using tcpdump, strings, and grep to investigate network traffic. By searching for specific strings and understanding protocol-specific patterns, they can identify relevant sessions and extract them for further examination.

2.4.2 Deep Packet Inspection

In network forensics, having a good understanding of packet is a plus point for network analysts. Looking at the packet in details such as the payload of the packet, the IP address, the timestamp, and the protocol can give a lot of useful information for the analyst to make a correlation of the incident and find more evidence. This technique is called deep packet inspection, a technique that involves inspection of data beyond the header of the packet such as the payload (Sikos, L.F., 2020). An analysis method called ‘string analysis’ that examines the packet for unique numeric and alphabetic characteristics (Parsons, C., 2012). In the same paper also stated that deep packet inspection is deployed in an equipment. This equipment will capture the packet and do the deep packet inspection process.

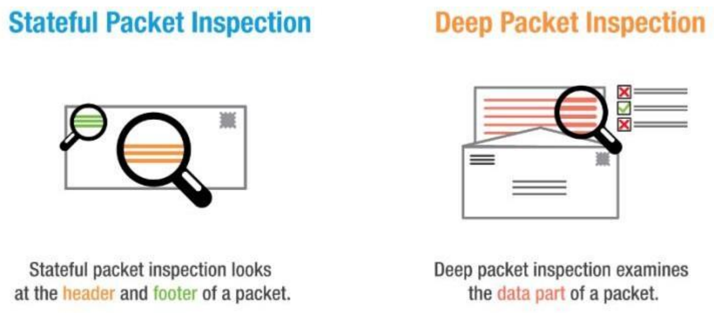
Stateful Packet Inspection
Deep Packet Inspection
Stateful packet inspection looks at the header and footer of a packet.
Deep packet inspection examines the data part of a packet.

Figure 2.1 Different between stateful and deep packet inspection

(Source: pages.moxa.com)

Deep Packet Inspection (DPI) involves examining all layers of network traffic, including headers and payload, for various purposes. By utilizing DPI, it becomes feasible to detect recognized malware signatures and identify network anomalies that may indicate potential attacks. This comprehensive inspection enables the determination of the source IP of an attack, identification of payload irregularities, and understanding the intentions and objectives behind network traffic. When combined with network flow analysis, DPI becomes a powerful tool for comprehending the sequence of an attack, uncovering the steps taken by an attacker, and identifying the utilization of different techniques. Additionally, DPI facilitates the evaluation of new exploitation methods within networks, enabling researchers to develop novel defense mechanisms and signatures (Pimenta Rodrigues, G. et al, 2017).

Other than that, the inspection of application level is also a good technique for network forensics. For HTTP protocol, identifying paths and parameters within URLs is a crucial requirement that enables the application of attribute-specific web attack detection models to modern web applications. Additionally, it serves as the initial stage in web application profiling, facilitating the detection of malicious activity that happens against websites (Minh, D.P. et al, 2017).

Overall, DPI is an efficient method for analyzing network traffic, identifying application-level attacks, giving information about potential threats, and helping to develop preventative protection measures.