International Journal of Engineering & Technology, 7 (4.17) (2018) 85-88

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Hybrid Pcap Analyser using T-Shark a tool that Makes use of Open Source Analyser that Can Meet Industrial Standards.

Dr G Pradeepini [1], G Muni Sai[2*], V Aruna[3]

[1]*Professor, Department of Computer Science and Engineering, Koneru Lakshmiah Deemed to be University.*
[2]*M.Tech Student, Department of Computer Science and Engineering, Koneru Lakshmiah Deemed to be University.*
[3]*Professor, Department of Computer Science and Engineering, Srinidhi Institute of Science and Technology*
**Corresponding Author Email: munisai555@gmail.com*

Abstract:

In general, Pcap file contains the network packets that are captured by the packet capture tool such as Wireshark, tcpdump, TShark etc. PCAP files can be obtains by intercepting network packets that are transmitted in the network. The use of PCAP is that the network investigator can be able to transfer the entire network data in a single file and it can also be used for Future analysis. This paper is about a method that can parse PCAP files in a new approach by reducing the time taken to investigate the PCAP file in multiple ways and this is done by parsing pcap which makes use of existing open source packet analyser. In order to achieve this method, I have developed a tool and the main feature of this tool is that it can be installed in one system and can be used in many systems within an organisation.

Keywords: *Packet Analyser, PCAP Parser, PCAP investigation, Packet Analysis, Network monitoring, Tshark, python, python-flask.*

I. Introduction:

As the Organization grows, the intranet within the organization grows as well which makes hard time for network administrator to monitor and deal with each and every network activity that is g present in the organization's Network. Network administrator must monitor and analyse each and every internal traffic packet that are hopping in the company in order to handle the network effectively and immediately tries to resolves the issues if any occurred. To ensure the security within the network, An Efficient Network Monitoring and packet analysis is required [1] and in most of the cases, Network Administrators may choose to save the pcap files for further forensic analysis or off-line analysis where they need a pcap analyser to parse the pcap file and expect some better and easy-to-understand output results [2].

1.1 Importance of Network Monitoring

Network Monitoring is a process where the Network administrators monitor each and every corner of internal network inside an organization [3]. This is to ensure that the network inside the organization and the organization itself is secure. Since network monitoring is a difficult task, it is considered as a vital part of Network Administrator Role. If Any Network Administrator fails to identify the malicious activities in the Network then the Network may have to deal with huge trouble and the name of the Organization as well its reputation will be in danger.

1.2. Importance of Network Analysis

One of the most important task of the network Administrator is to analyse the network traffic efficiently. There may be some situations where the Network administrator should capture the entire network traffic and place it aside so that it can be used for further analysis. Usually network Administrators captures internal network traffic and saves it in a file because it can be very difficult to manage and monitor huge number of network packets at the same time.

1.3. Importance of Packet Analysis.

Apart from capturing the network traffic, Network Administrator importance comes whiles analysing the captured packets. If the network administrator ever encounters a network problem inside a network, they usually start their analysis by trying to identify the source of the problem. Usually network administrators try to analyse important aspects of network like IP Address of both source and client, DNS servers, MAC address, Protocol Information, ports etc. and these basic information is enough to deal with most of the problems but clearly in sufficient while dealing with complex network problems.

1.4. Proposing Model Vs other Models

While monitoring the live network traffic, Network administrators need to analyse the pre-saved packet captures and they need to make sure that the analysis must be performed offline and this should not disturb the live capturing/monitoring process. There are a lot of open source and commercial tools that are available to perform PCAP analysis and this list contains various popular tools like Wireshark, Tshark, and Network miner. Wireshark is one of the most used open source packet capturing and PCAP analysis tool which has several abilities like search for certain Ports, Filtering various Protocols, IP Address, DNS and other filter options.

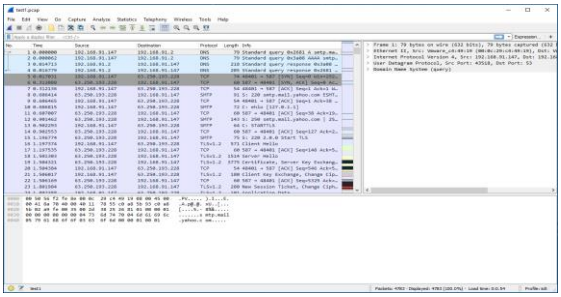

Figure 1.1: Analysing a pcap file using Wireshark.

Another product from Wireshark team is "Tshark" which is also an open source packet capture and packet analysis tool. TShark can perform almost everything that Wireshark does but the only difference between the both is that Wireshark contains GUI (Graphical User Interface) where as TShark is of Command line Interface [4]. In simple terms, TShark can be defined as the Command Line Version of Wireshark and Wireshark can be defined as the Graphical user Interface version of Tshark whose performance stands identical.

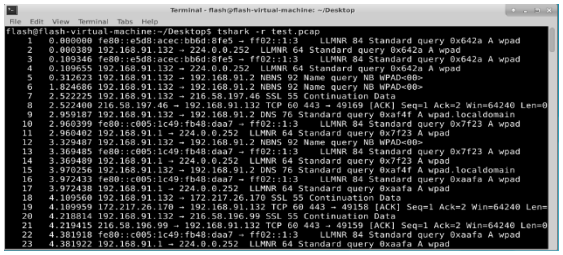

Figure 1.2: Analysing a pcap file using TShark from windows command prompt.

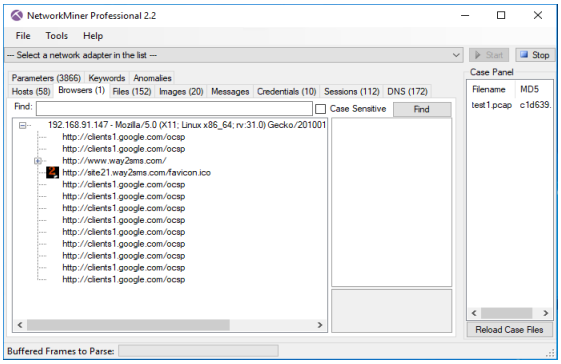

Figure 1.3: Analysing pcap file using network miner- A commercial tool to monitor and analyse network traffic.

2. Related Work:

In-order to parse the PCAP, we need to understand the encoding standards that is behind PCAP format [5] [6]. Standard pcap API is written in C Languages and we may need to use wrapper for other languages like Java [7], .NET [8], Python [9] and other Scripting languages. The best way to parse the PCAP without API is to use command line PCAP parsers. For example, TShark has everything that Wireshark does but only in Command Line Interface. We can make use of TShark Command line output and pass the entire raw data to the desired program to re-standardize based on requirement. Then later we can format the output in our desired way.

3. Proposed Model:

We need a method where we can make use of Network miner's categorization and Wireshark's various search/filter mechanism and in such a way that each and every scan that is performed with-in the organization stays in the organization or its own cloud. We need to make sure to export required results in several formats so that each and every one can get good grasp at the results after watching the output itself. We may need a menu for customizing our results so that we can violate details which may not necessary for our process.

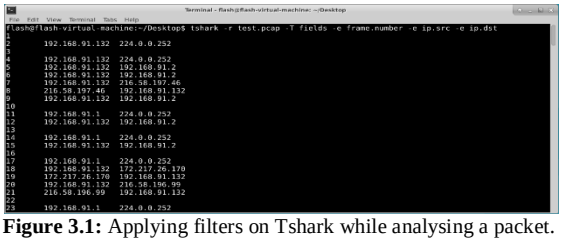

Figure 3.1: Applying filters on Tshark while analysing a packet.

Figure 3.1 contains command prompt where TShark is used to parse pcap file named test1.pcap to extract ip.src which is source IP and ip.dst which is Destination Fields. TShark contains several lot of options to extract Frame number, Source IP Address, Source Port Number. Destination IP Address, Destination port Number, Source MAC Address, Destination Mac Address, DNS, Frame length and anymore. We can get all those Extracted values in Command Prompt. The command which are used in the Figure 3.1 are
"tshark -r test.pcap -T fields -e frame.number -e ip.src -e ip.dst"

Where tshark is used to execute tshark,
-r specifies to read certain file
Test.pcap is the name of the file
-T indicates the format of text output and here we are using fields
-e indicates that it's a field to print
Ip.src – IP Source Address
Ip.dst – IP Destination Address [10]

Tshark allows us to use wide range of filters and fields and by making use of those options which are captured in plain text and are prettified by the help of python programming language. By the help of flask – a python web framework, we can convert terminal/command line-oriented python variable output to new and interactive Web based projection where we can able to check all the parsed outputs from the web browser itself.

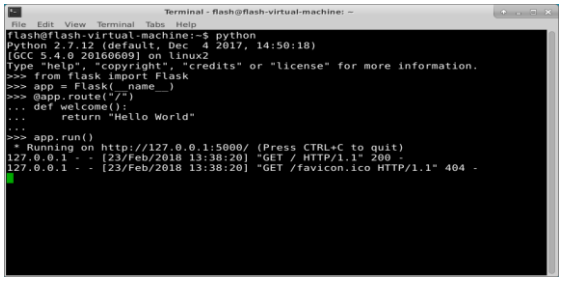

Figure 3.2: Executing a simple python-flask script from the python interpreter [11]

Figure 3.2 contains the execution procedure of simple flask server from the terminal and its output can be seen in the Figure 3.3.

Figure 3.3: Output for the python-flask script which was written in the figure 3.2

Here, Flask contains a decorator which is linked with a method and return. Here return is used to return either plain texted data or to render any html webpage .We need the decorator to present the data and through which we can manage/create new URL's and the contents that we need to display on that particular URL. Since Flask is very light and simple to use web framework among all python web servers. Flask makes use of jinja2 to render html pages.

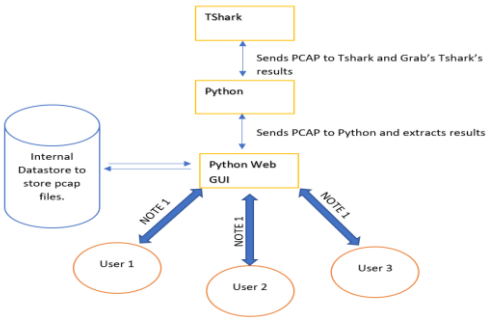

Figure 3.4: Working Procedure of this model

Note1: User 1/2/3 Interacts with Python -Flask Web GUI and provides either new PCAP file or select existing pcap file (from the data store) to the Python Flask server which passes the PCAP to Tshark. Once Tshark does all the work, it provides data back to the python variable where it is categorized and arranged so that User can understand them easily.

4. Execution:

Python Flask output can be seen in the Figure 4.1 where User is allowed to upload his/her desired pcap file or he/she can select an existing PCAP files from the local server storage.

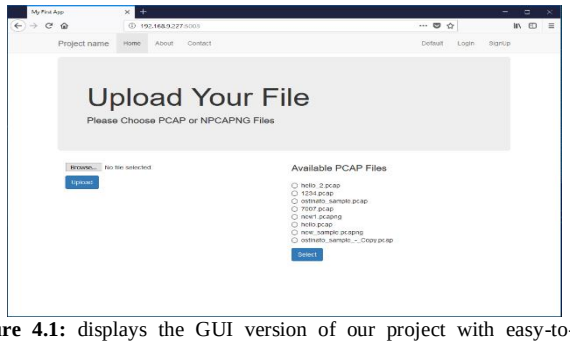

Figure 4.1: displays the GUI version of our project with easy-to-use interface which is hosted on our local machine.

Since the complete setup is based on Web GUI, it can be very easy to understand and almost any user who has some basic internet surfing abilities can be able to analyse the pcap file. All they need to do is to upload the given PCAP file

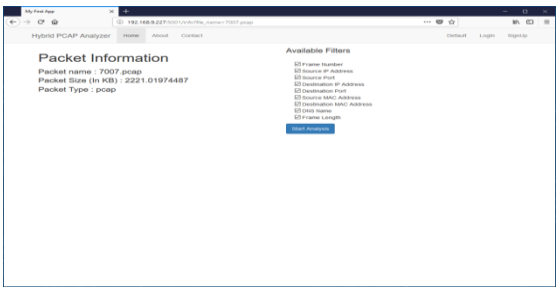

Figure 4.2: Filter Selection Panel

Once the user selects any one of either upload/select option from their selection panel, they will be migrated to Packet Information Screen where all the basic details which includes file name, file size, file type, file hash and user has the ability to select Filters from all the available filters and the available filers are

- Frame Number
- Frame IP Address
- Source Port
- Destination IP Address
- Destination Port
- Source MAC Address
- Destination MAC Address
- DNS Name
- Frame length

Once the user selects their required filters, the next page that awaits them is the Analysis Page as given in the Figure 4.3

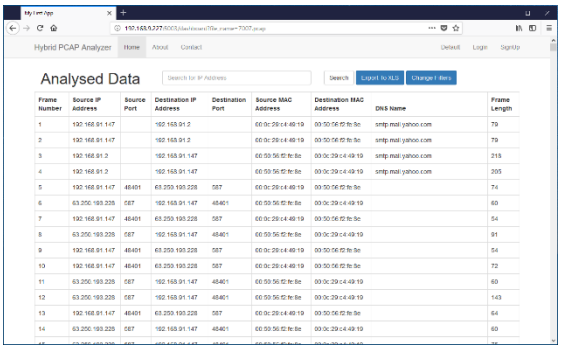

Figure 4.3: contains the analysed data which are arranged according to their category which can be easier to understand when compared to that of Wireshark.

5. Advantages of Proposed Model over Existing Models:

Wireshark is reliable in most of the cases and in-depth understanding of Wireshark is recommended along with several search and filter commands in order to perform analysis effectively which may cost administrators time.

- We need to install Wireshark (/or TShark) on each and every system to analyse the packet and we can neither export results nor store results whereas This Model can be installed in one machine and it can be accessible from various other machines with the help of network.
- This Model allows us to save analysed pcap file and its results as well so that we can able to access those results anytime in the future.
- Each and Every case (Analysis) is stored in their respective databases so that we can be able to export the DB file effectively. There are other export options available which allows investigator to generate their results in the form of CSV or Excel files.
- This method makes use of authentication to separate pcap/analysis from each other and Admin or Administrator group members have the ability to view pcap or results of the respective pcap of any user.
- Very interactive web client to manage and work easily.

6. Conclusion:

In this paper, we have seen the various ways to make use of existing Tshark tool to develop a new interactive multi-feature tool which can analyse the pcap/pcapng files just as any commercial tool with extra features and advanced customized facility so that user can decide his/her own way to generate and export analysed outputs. We are also managed to include a-cloud-like feature where Hybrid PCAP Analyzer can store the previously searched pcap files and its results as well. This paper proves that

an existing open source can be reused to match present industry standards and we can manage to minimize the cost of commercial tools. By installing it in one machine, we can able to analyse multiple number of packets from multiple machines in single time. Since this tool completely works online, any sensitive data of that organization will stay in that particular organization itself.

References

[1] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Muhammad Inayatullah Babar "An Efficient Network Monitoring and Management System"
[2] https://www.sans.org/reading-room/whitepapers/forensics/forensic-timeline-analysis-wireshark-giac-gcfa-gold-certification-36137
[3] https://www.wireshark.org/docs/wsug_html_chunked/AppToolstshark.htmlx
[4] David E Morgan, Walter Banks, Dale P Goodspeed Richard Kolanko "A Computer Network Monitoring System"
[5] V. Veselý: Extended Comparison Study on Merging PCAP Files
[6] An Efficient PCAP Extraction Tool- international Journal of Advanced research in Computer Science and Software Engineering
[7] http://www.javahelps.com/2017/08/parse-pcap-files-in-java.html
[8] https://www.codeproject.com/Articles/12458/SharpPcap-A-Packet-Capture-Framework-for-NET?msg=5428440
[9] scapy: https://scapy.readthedocs.io/en/latest/
[10] https://www.wireshark.org/docs/man-pages/tshark.html
[11] Flask is Fun : http://flask.pocoo.org/