Computer Network Analysis for a Network User Behaviour: A Case Study of Buildings PPBS D Jatinangor

Drs. Ino Suryana, M.Kom.[#1], Rudi Rosadi, S.Si., M.Kom.[#2], Deni Setiana,S.Si., M.CS[#3], Izzan Lastryana Oktiadi[#4]

[#]*Department of Computer Science, Padjadjaran University*
Sumedang, 45363, Indonesia

Abstract: *Computer networks are widely used for various purposes. User of computer networks need to be analyzed, to determine how effective the computer network is used. Network forensics plays an important role to transform the data packet into a structure that can be understood for further use. Packet sniffing process took the entire packet on the network, the classification used here is the port and protocol. In this thesis carried out the manufacture of desktop-based network tools using Visual Studio 2013 and C # programming language. Tools can classify network users with data sources .pcap format. Based on the test results, resulting that HTTP / HTTPS is active in wireless and wired than already access the website / server that leads to education. VPN is more active than the wired LAN. Dropbox is widely used on wired or wireless networks. Based on bytes in Wednesday on the wireless and wired is the highest compared to other days. Based on the IP header length no attack happened.*

Keywords: *Computer Network, Network Forensic, Port, Protocol, Packet Sniffing*

I. INTRODUCTION

In the current era, the network for accessing the Internet becomes a primary need that is needed by many people. In networks, data flows and network user information has it got from the local network or from the Internet. This data can be utilized in order to determine the activities of its users and to see how effective the network is used, so that the network will form a pattern that is useful for the future.

Network forensics is a branch of digital forensics that focuses on the monitoring and analysis of network traffic. The goal is tracking and monitoring traffic of network to make sure of how an attack took place [1].

Packet sniffing, the process of capturing the information transmitted across network. Packet Sniffing mainly used in network management, monitoring and ethical hacking. To perform sniffing we use tool named packet sniffer [2].

Packet sniffer is a program running in a network attached Device that passively receives all data link layer frames passing through the device's network adapter [3].

This research will explore the analysis of computer network using classification port and protocol method which will show information about how effective computer network is used.

II. LITERATURE REVIEWS

2.1 Computer Network

The computer network (computer network) is a collection of two or more computers, each of which stands alone and is connected through a technology that can exchange information [4]. Computers that can connect via cable transmission medium (wired) or wireless. Examples of transmission media cable (wired), namely copper cable, fiber optic. Examples of transmission media wireless, namely infrared, bluetooth, wifi, satellite.

2.2 Network Forensic

Network forensics is the process of collecting, recording, and examining of network events for finding the source of security attacks. It helps in identifying unauthorized access to computer systems, and searches for evidence in case of such an occurrence. Network forensics is in fact to investigate, at a network level, things taking place or that have taken place across an IT system [1].

2.3 Packet Sniffer

Packet sniffer is a program running in a network attached Device that passively receives all data link layer frames passing through the device's network adapter. It is also known as Network or Protocol Analyzer or Ethernet Sniffer. The packet sniffer captures the data that is addressed to other machines, saving it for later analysis. It can be used

legitimately by a network or system administrator to monitor and troubleshoot network traffic [3].

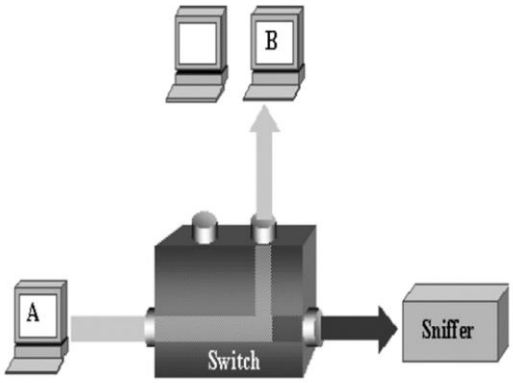

Fig. 1 Process Sniffing

2.4 TCP and UDP port number

TCP and UDP port number is divided into three:

- Well known port numbers
  Controlled and assigned by the IANA and most systems can only be used by root or the program is run by privileged users. Port number 0 – 1023 [5].

- Registered port numbers
  Registered ports are not controlled by the IANA and on most systems can be used by ordinary users or programs executed by ordinary users. Port number 1.024 - 65.535 [5].

- Dynamic, private or ephemeral ports
  This port is in the range of 49.152 – 65.535 containing dynamic and private ports that are not registered with IANA. Normally used for personal, services or temporary purpose [6].

2.5 IP header detection

IP header length in the IPV4 must be equal or above 20 bytes and equal to or below 60 bytes. If the IP header length is less than 20 bytes or 60 bytes above, it can be suspected that there is an attack contained in a computer network [7].

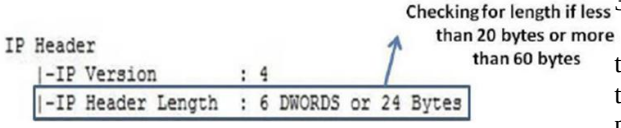

Fig. 2 The normal length of the IP header

III.RESEARCH METHODOLOGY

3.1 Research Data

Data were collected using netsniff-ng application on Kali Linux commands typed at the terminal for data retrieval is done during the month. The command I use in data collection:

1. Wired

netsniff-ng --in eth0 --out /folderdestination –silent --bind-cpu 0 --interval 24hrs

2. Wireless

netsniff-ng --in wlan0 --out /folderdestination –silent --bind-cpu 0 --interval 24hrs

3.2 Software Development

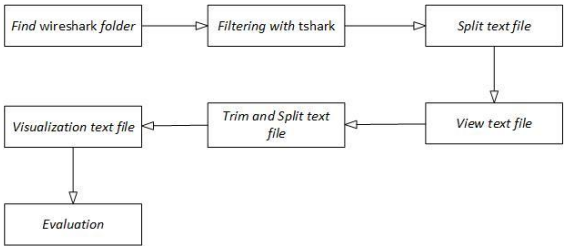

Figure 3 Block diagram analyzer software.

3.2.1 Find wireshark folder

The process aims to find the folder wireshark find tshark programs that are in a folder wireshark. If available, the analysis process can be done, if it has not then the process will continue and be required to install wireshark program first.

3.2.2 Filtering with tshark

This process separates the packet contained in the data based on port and protocol. Port to be analyzed is 1 to 1023, 1900 and 17500. As well as the number of packets / frames and bytes based on the protocol contained in the data. Once separated and then stored in the form of text files (.txt).

3.2.3 Split text file

The process needed to split text file text file that contains the data that has been filtered, can be displayed according to the format given and certainly readable.

3.2.4 View text file

This process displays view text files that have been processed split text files on a data grid view on the application. The view can be changed in accordance with the selection of filters available on the application.

3.2.5 Trim and Split text file

This process of cutting and separation so that the captured data can be visualized. The data taken is the protocol name, the number of frame / packet and the number of bytes.

3.2.6 Visualization text file

This process changed the protocol name, the number of frame / packet and bytes into a graph. Protocol name used for the x-axis and the number of frames / packets and bytes are converted to an integer is used for the y-axis.

3.2.7 Evaluation

Process evaluation was conducted to determine the application has been in line with expectations, and can take an early conclusion to do further analysis.

IV. IMPLEMENTATION AND RESULTS

4.1 Implementation Constraints

Limitations in this research are:
1. Applications can only handle data packet capture format (.pcap) for data analysis and visualization of data.
2. Application only supporting analysis tools, for weekly or monthly analysis takes the process further.

4.2 Implementation System

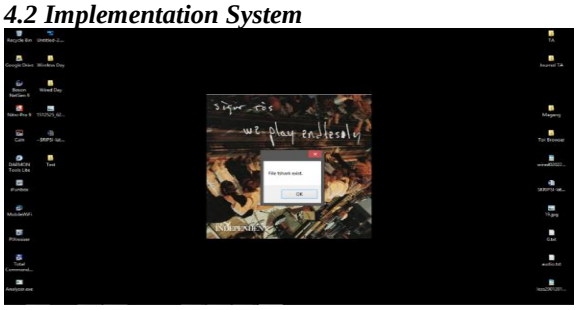

Figure 4 Search programs tshark

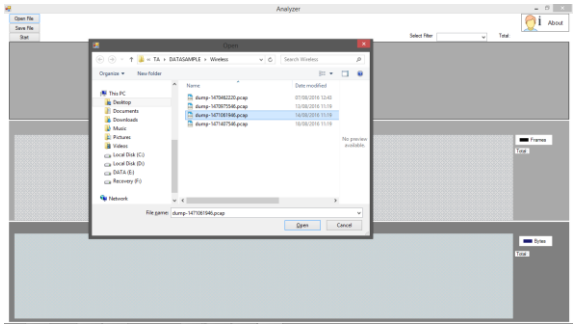

Figure 5 Display for selecting data .pcap

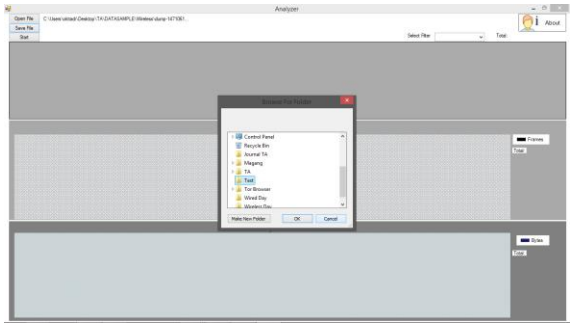

Figure 6 Display for the destination folder

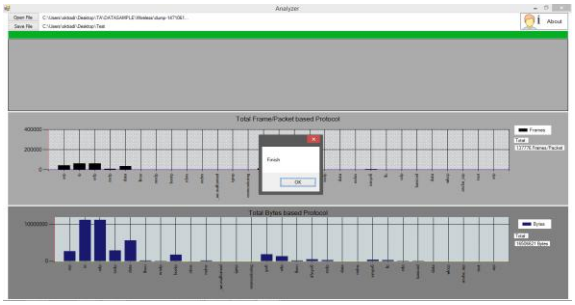

Figure 7 Display filtering process has been completed.

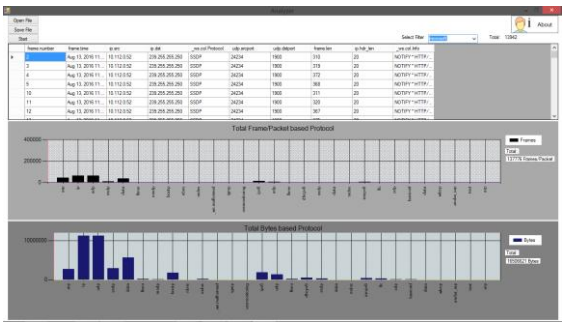

Figure 8 Display overall results.

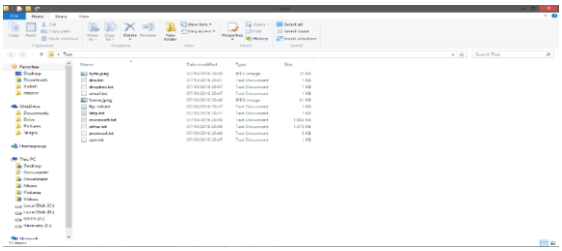

Figure 9 The results in the folder.

4.3 Analysis of Results of Testing

In testing using the data 32 PCAP cable (wired) and 32 Data PCAP (wireless) are classified by port, protocol and packet header length per day which is then reprocessed to analyze network users on building PPBS D, Jatinangor.

4.3.1 Port

- HTTP

HTTP / HTTPS authors classify is the destination or source port 80, 443, or 8080. The results of the analysis of data during the month that the comparison between wired and wireless from day to day.

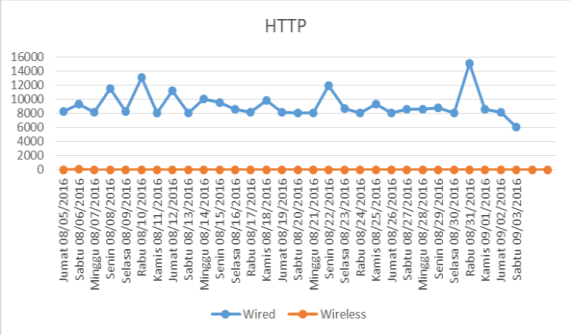

Figure 10 Graph view HTTP / HTTPS for a month from day to day.

From Figure 10 it can be seen that the access of HTTP / HTTPS are the highest wired occurred on August 31, 2016, which reached 15100 requests, and on other days ranges from 8000 to 11000 requests. While on wireless only nine requests for HTTP / HTTPS for a month.

Table I Results of access HTTP / HTTPS highest on wired for a month

No	Website/Server	Total Access
1	Teamviewer	152790
2	IEEE	3999
3	Amazon Web Service	1438
4	Google	1363
5	Facebook	97

- Dropbox

Dropbox is the author classifies the destination or source port 17500. The results of the analysis of data during the month that the comparison between wired and wireless from day to day.

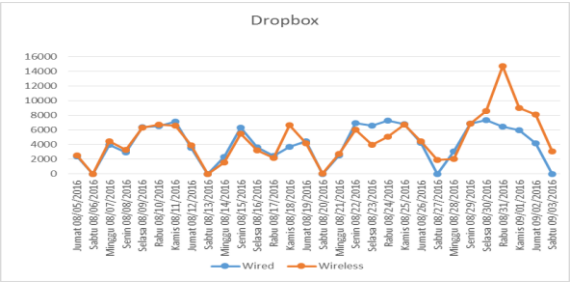

Figure 11 Graph of views Dropbox for a month from day to day.

Dropbox users is quite high in the building PPBS D, Jatinangor the range 4000 to 7000 requests per day either in wired or wireless. Dropbox users to decline until there is no demand every Saturday on the first Sunday, the second and third. On the fourth Saturday and Sunday there is a difference of use of the three previous week on the wireless in the range of 2000 demand. The highest usage in the wireless Dropbox occurred on August 31, 2016 with the request 14741 and the wired occurred on August 30, 2016 with 7352 requests.

- Microsoft port

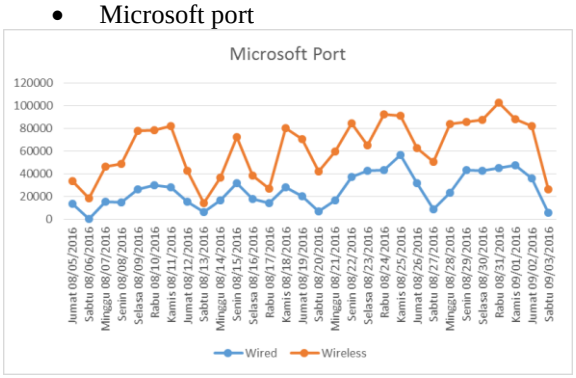

Figure 12 Graph of views Microsoft Port for a month from day to day.

Microsoft ports authors classify is the destination or source port 1900. The results of the analysis of data during the month that the comparison between wired and wireless from day to day.

From Figure 12 seen wireless and wired users on a Microsoft port is port 1900 (UDP) is quite high. Microsoft is part of SSDP port normally used for advertising, information display and includes network services. In 2014 the port 1900 is used for DDoS attacks by sending packets at the IP with a large number. From these cases, the author wants to analyze the port in 1900, there are attacks like the above case. It turned out that after analysis there was no attack on this port. Highest user port 1900 on wireless occurred on August 31, 2016 to demand 102 553 and the wired occurred on August 25, 2016 with 56 528 requests.

- Other

Other ports are authors classify is the destination or source port 1 until 1023 and not port 80, 443, 8080, 53, 21, 22, 23, 25, 110, 143, 587, 465, 993, 995, 500, 465 and 443 (SSL). The results of the analysis of data during the month that the comparison between wired and wireless from day to day.

In Figure 13 seen changes from day to day and erratic changes. But every Saturday decline and rise again on Sunday. This affects the number of users, the more users, the more the demand of port. The highest demand on wired occurred on August 15, 2016 with 78 944 requests and on a wireless occur on 1 September 2016, with 61 637 requests.

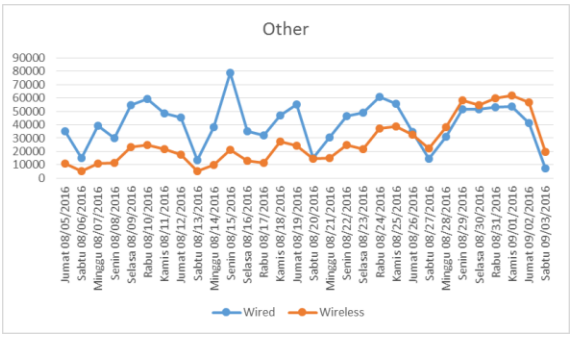

Figure 13 Graph Other views during the month from day to day.

- VPN

VPN (virtual private network) that authors classify is the destination or source port 500, 1701, 4500, 1723, 465 and 443 (SSL). The results of the analysis of data during the month that the comparison between wired and wireless from day to day

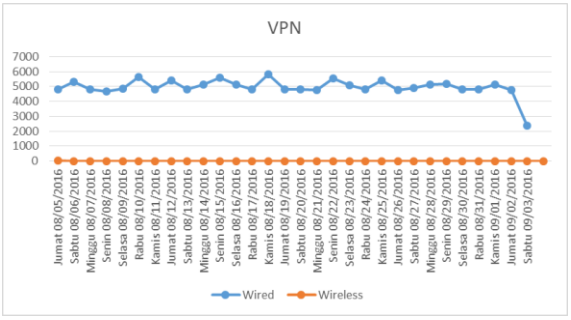

Figure 14 Display VPN for a month from day to day.

In Figure 14 shows that the VPN users are on a wired network while on the wireless network there is no demand VPN. VPN allows you to access the Internet via other networks, typically to access a website or application that is blocked by the server. Highest user VPN access to the wired occurred on August 18, 2016 with 5820 requests.

- DNS, Email, FTP, SSH

1. DNS

DNS (domain name server) that the authors classify is the destination or source port 53. The results of the analysis of data during the month that the comparison between wired and wireless reveals no DNS requests to both wired and wireless.

2. Email

Email the author classify is the destination or source port 25, 110, 143, 587, 465, 995 and 993. The results of the analysis of data during the month that the comparison between wired and wireless turned out there were only 20 requests email which occurred on 2 September 2016 in wired.

3. FTP and SSH

FTP (file transfer protocol) and SSH (secure shell) that the authors classify is the destination or source port 21, 22, 23. The results of the analysis of data during the month that the comparison between wired and wireless was not found a request to the FTP and SSH both wired and wireless.

4.3.2 Protocol

Day	Wired	Wireless
Monday	UDP	UDP
	LLMNR	DATA
	NBNS	ARP
UDP bytes	20.000.000 - 38.000.000	90.000.000-110.000.000
UDP data bytes	3.000.000 - 5.000.000	40.000.000 - 65.000.000
Tuesday	UDP	UDP
	BOOTP	DATA
	HTTP	SSDP
UDP bytes	30.000.000 - 41.000.000 Except Week 2: 20.000.000	80.000.000 - 120.000.000 Except Week 2: 40.000.000
UDP data bytes	1.000.000 - 5.000.000 Except Week 2: 1.000.000	50.000.000 - 60.000.000 Except Week 2: 23.000.000
Wednesday	UDP	UDP
	BOOTP	Data
	HTTP	ARP
UDP bytes	31.000.000 - 40.000.000 Except Week 2 23.000.000	90.000.000 - 120.000.00 Except Week 2 23.000.000
UDP data bytes	3.000.000 - 10.000.000 Except Week 2 2.000.000	50.000.000 - 60.000.000 Except Week 2 13.000.000
Thursday	UDP	UDP
	HTTP	DATA
	BOOTP	ARP
UDP bytes	30.000.000 - 39.000.000 Except Week 2 28.000.000	90.000.000 - 110.000.000
UDP data bytes	5.000.000	about 60.000.000
Friday	UDP	UDP
	HTTP	DATA
	BOOTP	ARP
UDP bytes	20.000.000 - 30.000.000	100.000.000 - 110.000.000 on Week 3,4,5. Except Week 1,2 30.000.000 - 40.000.000
UDP data bytes	2.000.000 - 3.000.000	50.000.000 - 60.000.000 on Week 3,4,5. Except Week 1,2 20.000.000 - 30.000.000
Saturday	UDP	UDP
	Data	ARP
total packets	30.000 - 40.000	Week 1 and 2 :50.000 packet With 10.000.000 bytes Week 3 UDP: 380.000 packet With 75.000.000 bytes Week 4 UDP: 400.000 packet With 80.000.000 bytes
bytes per protocol	20.000.000 bytes	Week 5 UDP : 200.000 packet With 40.000.000 bytes
Sunday	UDP	UDP
total packets	40.000 - 50.000	Week 1 UDP: 200.000 packet With 30.000.000 bytes Week 2 UDP: 180.000 packet With 28.000.000 bytes Week 3 UDP: 400.000 packet With 80.000.000 bytes
bytes	20.000.000 - 28.000.000	Week 4 UDP : 500.000 packet With 100.000.000 bytes

Figure 14 Display result based protocol.

- Monday

1. Wired

On Monday in wired, UDP total bytes in between 20,000,000 to 38,000,000 bytes, and total bytes of data UDP between 3,000,000 to 5,000,000 bytes.

2. Wireless

On Monday in wireless, UDP total bytes ranging from 90,000,000 to 110,000,000 and UDP bytes of data ranging from 40,000,000 to 65,000,000 bytes.

- Tuesday

1. Wired

On Tuesday in wired, UDP total bytes in between 30,000,000 to 41,000,000 bytes except Week 2 is 20,000,000 bytes and total bytes of data UDP bytes ranging from 2,000,000 to 5,000,000 bytes except Week 2 of 1,000,000 bytes. There was a decline for tomorrow's holiday is August 17, 2016.

2. Wireless

On Tuesday in wireless, UDP total bytes ranging from 80,000,000 to 120,000,000 bytes except Week 2 were approximately 40,000,000 bytes and total bytes of data UDP ranged between 50,000,000 to 60,000,000 bytes except Week 2 is 23,000,000 bytes. There was a decline for tomorrow's holiday is August 17, 2016.

- Wednesday

1. Wired

On Wednesday in wired, UDP bytes in total approximately 31,000,000 to 40,000,000

bytes except Week 2 is 23,000,000 bytes and total bytes of data UDP range from 3,000,000 to 10,000,000 bytes except Week 2 of the 2,000,000 bytes. In Week 2 decrease due to public holidays, namely August 17, 2016.

2. Wireless

On Wednesday in wireless, UDP total bytes ranging from 90,000,000 to 120,000,000 bytes except Week 2 that about 23,000,000 bytes, and total bytes of data UDP ranges from 50,000,000 to 60,000,000 bytes except Week 2 is 13,000,000 bytes. Week 2 decrease due to public holidays, namely August 17, 2016.

- Thursday

1. Wired

On Thursday in wired, UDP total bytes in between 30,000,000 to 39,000,000 bytes except Week 2 is 28,000,000 bytes and total bytes of data UDP ranges from 5,000,000 bytes. Week 2 decline since early entry after holiday August 17, 2016.

2. Wireless

On Thursday in wireless, UDP bytes total around 90,000,000 to 110,000,000 bytes, and total bytes of data UDP range 60.000.00 bytes.

- Friday

1. Wired

On Friday in wired, UDP bytes total around 20,000,000 to 30,000,000 bytes, and total bytes of data UDP range from 2,000,000 to 3,000,000 bytes.

2. Wireless

On Friday in wireless, UDP total bytes ranging from 100,000,000 to 110,000,000 bytes at weeks 3, 4 and 5, while at weeks 1 and 2 ranges from 30,000,000 to 40,000,000 and the total bytes of data UDP ranges from 50,000,000 to 60,000,000 bytes at weeks 3, 4, and 5, while at weeks 1 and 2 ranges from 20,000,000 to 30,000,000 bytes. Improvement that occurred at weeks 3, 4 and 5 occur because it started early lectures.

- Saturday

1. Wired

On Saturday in wired seen every Saturday at wired visible difference with Monday through Friday because instead of working days which resulted in traffic that occurs is very low. Seen from the number of packets / frames in between 30,000 to 40,000 packet every week and the total bytes per protocol does not exceed 20,000,000 bytes.

2. Wireless

On Saturday in wireless, weeks 1 and 2 traffic is still low seen from the number of frames / packets in the range of 50,000 and the highest total at 10,000,000 bytes. In week 3, 4, 5 and the highest increase at week 4. At week 4 UDP packet reach 400,000 and bytes total 80,000,000 bytes. At week 3 UDP packet reach 380,000 and bytes total 75,000,000 bytes. At week 5 UDP packet reach 200,000 and bytes total 40,000,000 bytes. Improvement that occurred at weeks 3, 4 and 5 occur because it started early lectures.

- Sunday

1. Wired

On Sunday in wired, with the highest UDP packet requests ranging from 40,000 to 50,000 with a total of 20,000,000 to 28,000,000 bytes.

2. Wireless

On Sunday in wireless, Week 1 has a UDP ranges from 200,000 frames / packets and bytes total reached 30,000,000 bytes. At weeks 3 and 4 increases. At week 2 UDP packet with 180,000 and bytes total 28,000,000 bytes. At week 3 UDP packet to reach 400,000 and bytes total 80,000,000 bytes. At week 4 UDP reach 500,000 and bytes total 100,000,000 bytes. Improvement of Week 3 and 4 occur because it started early lectures.

4.3.3 IP header length

In this study the authors wanted to know from these data occur against network attackers to view the IP header length contained in HTTP / HTTPS, DNS, Dropbox, FTP and SSH, Microsoft Port, Email, VPN and Other Port. Normal IP header has a length of 20 bytes to 60 bytes, if lower 20 bytes or greater than 60 bytes then it would indicate that there is an attacker.

After the analysis there were no attacks on the network, the IP header length everything was normal to have a length of 20 bytes in the HTTP / HTTPS, DNS, Dropbox, FTP and SSH, Microsoft Port, Email, VPN and Other Port either in wired or wireless.

V. CONCLUSIONS

5.1 Conclusions

1. Analyzer successfully developed as a c# based networking tools.

2. HTTP / HTTPS is active in wireless and wired than already access the website / server that leads to education. VPN is more active than the wired LAN. Dropbox is widely used on wired or wireless networks.

3. Based on bytes in Wednesday on the wireless and wired is the highest compared to other days. Based on the IP header length is not an attack that happened.

5.2 Suggestions

1. Applications can be analyzed on a weekly or monthly as well as more ports that can be analyzed, making it easier to take a picture of network users.
2. Applications can be analyzed from a data source other than a packet capture (.pcap).
3. Applications can be developed based on mobile.

ACKNOWLEDGMENT

Our thank goes to Department of Computer Science, also Faculty of Mathematics and Science at Padjadjaran University, who has helped organize this research in Indonesia.

REFERENCES (SIZE 10 & BOLD)

[1] A. Srivastav, and I. Ali, "Network Forensics an emerging approach to an network analysis", International Journal of Computer Science & Engineering Technology (IJCSET), vol. 5 no.02, pp.118-123, Feb.2014.

[2] P. Asrodia, and V. Sharma, "Network Monitoring and Analysis by Packet", International Journal of Engineering Trends and Technology (IJETT), vol. 4 issue.5, pp.2133-2135, May.2013.

[3] P. Asrodia, and H. Patel, "Network Traffic Analysis Using Packet Sniffer", International Journal of Engineering Research and Applications (IJERA), vol. 2 issue.3, Pp.854-856, May-June.2012.

[4] Andrew S.T, Computer Networks 4th Edition, New Jersey: Prentice Hall, 2003.

[5] J. Reynolds, & J. Postel, "RFC 1700: Assigned Number". Internet Engineering Task Force (IETF), pp.15-55, Oct.1994.

[6] (2016) Wikipedia List of TCP and UDP port numbers. [Online]. Available: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

[7] I. Riadi, J. E. Istiyanto, A. Ashari and Subanar, "Internet Forensics Framework Based-on Clustering", (IJACSA) International Journal of Advanced Computer Science and Applications. vol. 4 no.12, pp.115-123, 2013.