

**Proceedings**



**CommNet**



## **2019 International Conference on Advanced Communication Technologies and Networking (CommNet)**

**ISBN : 978-1-5386-8317-0**

**Catalog Number: CFP19N84-ART**

**Editors:**

**Faissal El Bouanani**

**Fouad Ayoub**

**Paschalis C. Sofotasios**

**Daniel Benevides da Costa**

**Rabat, Morocco**

**April 12-14, 2019**

# Preface

It is our pleasure to introduce you to the proceedings of the International Conference on Advanced Communication Technologies and Networking (CommNet'19). The international conference was held during 12-14 April 2019 in Rabat, the capital city of Morocco. CommNet'19 was co-organized by ENSIAS college of Engineering, and the Association for Research and Innovation in Science and Technology (ARINST), with the partnership of IEEE Morocco section.

CommNet'19 by its second edition at a conference level attracted an important volume of submitted papers from various areas of communication systems, security and networking. Very warm thanks go to Professors Fouad Ayoub, Hussain Ben-azza, and El Alami Semma the General co-chairs of the conference, to the steering committee chairs led by Professors Daniel Benevides da Costa, George K. Karagiannidis, Mohamed-Slim Alouini, and Paschalis. C. Sofotasios, and to the Program Committee led by its chairs, Professors Daniel Benevides da Costa and Paschalis C. Sofostasios. A large number of submissions from different countries were received, among which, 40 papers, including 2 invited papers, have been accepted based on their timelines and relevance, novelty, technical content, and clarity of presentation, to be included in the proceedings. The conference program featured an opening and closing sessions, parallel paper sessions and two keynote presentations. Hearty thanks also go to the CommNet'19 partners, sponsors, keynote speakers and local organizers. We would like to thank everyone that has contributed in rendering the conference an extraordinary and enjoyable event. Last but not least, welcome back to CommNet'20 next year.

**Faissal El Bouanani**

Mohammed V University in Rabat, Morocco

General chair of CommNet'19

# The 2<sup>nd</sup> International Conference on Advanced Communication Technologies and Networking (CommNet'19)

## Honorary Chair:

- Mohamed Essaaidi, ENSIAS, Mohammed V University, Rabat, Morocco

## Steering Committee:

- Daniel Benevides da Costa, Federal University of Ceará, Brazil
- Faissal El Bouanani, ENSIAS, Mohamed V University, Morocco
- George K. Karagiannidis, Aristotle University of Thessaloniki, Greece
- Mohamed-Slim Alouini, KAUST, Kingdom of Saudi Arabia
- Paschalis. C. Sofotasios, Khalifa University of Science and Technology, UAE & Tampere University of Technology, Finland

## General Chairs

- Faissal El Bouanani, ENSIAS, Mohamed V University, Morocco (**General Chair**)
- Fouad Ayoub, CRMEF Kenitra, Morocco (**General co-Chair**)
- Hussain Ben-Azza, Moulay Ismail University, Meknes, Morocco (**General co-Chair**)
- El Alami Semma, FST Settat, Hassan I University, Morocco (**General co-Chair**)

## TPC Chairs

- Daniel Benevides da Costa, Federal University of Ceará, Brazil
- Paschalis. C. Sofotasios, Khalifa University of Science and Technology, UAE & Tampere

## Junior Committee

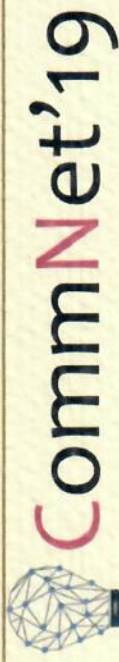
- Elmehdi Illi, ENSIAS, Mohamed V University, Morocco
- Mounia Bouabdellah, ENSIAS, Mohamed V University, Morocco
- Toufik Chaayra, ENSAM, Moulay Ismail University, Meknes, Morocco

# Table of Contents

|  |           |
|--|-----------|
| <b>Substitution Box Design Based on Chaotic Maps and Cuckoo Search Algorithm .....</b>   | <b>1</b>  |
| Tanveer Akhtar, Nizamud Din, Jamal Uddin   |           |
| <b>Physical-Layer Security over Generalized SIMO Multipath Fading Channels.....</b>  | <b>8</b>  |
| Jules M. Moualeu, Paschalis C. Sofotasios, Daniel Benevides da Costa, Walaa Hamouda, Ugo S. Dias, Sami Muhaidat  |           |
| <b>Network Traffic Monitoring and Analysis using Packet Sniffer .....</b>  | <b>14</b> |
| Apri Siswanto, Abdul Syukur, Evizal Abdul Kadir, Suratin   |           |
| <b>Smart Sensor Node of WSNs for River Water Pollution Monitoring System.....</b>  | <b>18</b> |
| Evizal Abdul Kadir, Apri Siswanto, Sri Listia Rosa, Abdul Syukur, Hitoshi Irie, Mahmud Othman  |           |
| <b>Adaptive Self-Interference Cancellation for Full Duplex Systems with Auxiliary Receiver .....</b>   | <b>23</b> |
| Maggie Shammaa, Hendrik Vogt, Ahmed E. El-Mahdy, Aydin Sezgin  |           |
| <b>A High Capacity Geometrical Domain Based 3D Image Steganography Scheme.....</b>   | <b>31</b> |
| Sara Farrag, Wassim Alexan   |           |
| <b>Secure 2D Image Steganography Using Recamán's Sequence.....</b>   | <b>38</b> |
| Sara Farrag, Wassim Alexan   |           |
| <b>BER Analysis in Relay-Based DF Cooperative Diversity Systems over Rayleigh Fading Channels with Non-Identical Interferers near the Destination.....</b> | <b>44</b> |
| Mamoun F. Al-Mistarihi, Rami Mohaisen, Khalid A. Darabkh   |           |
| <b>Packet Scheduling in 4G and Beyond Networks Using CrossLayer Design Approach... </b>  | <b>49</b> |
| Wisani Salani, Gbolahan Aiyetoro, Fambirai Takawira  |           |
| <b>On the Secrecy Analysis of Dual-Hop Underlay Multi-Source CRNs with Multi-Eavesdroppers and a Multi-Antenna Destination.....</b>                        | <b>55</b> |
| Mounia Bouabdellah, Faissal El Bouanani, Daniel Benevides da Costa, Paschalis C. Sofotasios, Hussain Ben-azza, Kahtan Mezher, Sami Muhaidat                |           |
| <b>Performance Analysis of a Smart Street Lighting application using LoRaWan.....</b>  | <b>62</b> |
| Yaye SARR, Bamba GUEYE, Cheikh SARR  |           |
| <b>Towards a Clustering-Based Approach to Speed up IaaS Services Discovery Process... </b>   | <b>68</b> |
| Driss RIANE, Ahmed ETTALBI   |           |
| <b>Routing-Plan duplicator: A reliable assistant for safe and seamless migration toward SDN .....</b>  | <b>73</b> |

Madjed BENCHEIKH LEHOCINE, Salim DJAABOUB, Mohamed BATOUCHE

|  |            |
|--|------------|
| <b>An Importance Sampling Method for Monte-Carlo Integration Model for Ultraviolet Communication.....</b>  | <b>83</b>  |
| Renzhi Yuan, Jianshe Ma, Ping Su, Yuhan Dong, Julian Cheng   |            |
| <b>Optimal Decision on Placement of an Auxiliary Aerial Wireless Base Station Using the Artificial Bee Colony Algorithm .....</b>                    | <b>89</b>  |
| Ashraf Tahat, Talal Edwan, Dana Mbaideen, Nada Murrar, Ola Al-Qutob, Leen Ayman  |            |
| <b>Automated trust negotiation for Cloud applications in Identity-as-a-Service.....</b>  | <b>95</b>  |
| Tri Hoang Vo, Woldemar Fuhrmann, Klaus-Peter Fischer-Hellmann, Steven Furnell  |            |
| <b>A Meter Band Rate mechanism to improve the native QoS capability of OpenFlow and OpenDaylight.....</b>  | <b>103</b> |
| Mohamed Saleh Al Breiki, Suiping Zho, Yuan Roger Luo   |            |
| <b>Improve R2L Attack Detection using Trimmed PCA.....</b>   | <b>109</b> |
| ELKHADIR Zyad, ARCHI Taha, BENATTOU Mohammed   |            |
| <b>PAPR reduction in MIMO-OFDM based on Polar Codes and Companding technique .....</b>   | <b>114</b> |
| Brahim BAKKAS, Idriss CHANA, Hussain BEN-AZZA  |            |
| <b>Triple-Layer Image Security Using a Zigzag Embedding Pattern.....</b>   | <b>120</b> |
| Sara Farrag, Wassim Alexan, Hisham H. Hussein  |            |
| <b>Double-Layer Image Security Scheme With Aggregated Mathematical Sequences.....</b>  | <b>128</b> |
| Marwa Tarek Elkandoz, Wassim Alexan, Hisham H. Hussein   |            |
| <b>An access authentication algorithm based on a hierarchical identity-based signature over lattice for the space-ground integrated network.....</b> | <b>135</b> |
| Zhuo Yi, Xuehui Du, Ying Liao, Xin Lu  |            |
| <b>A Clever Approach to Develop an Efficient Deep Neural Network Based IDS for Cloud Environments Using a Self-Adaptive Genetic Algorithm.....</b>   | <b>144</b> |
| Zouhair Chiba, Noredine Abghour, Khalid Moussaid, Amina El omri, Mohamed Rida  |            |
| <b>Receiver Design for Dual-Mode Index Modulation Aided OFDM.....</b>  | <b>153</b> |
| Yusuf Acar, Sultan Aldırmaz Çolak  |            |
| <b>Managing Security Policies within Cloud Environments Using Aspect-Oriented State Machines .....</b>   | <b>158</b> |
| Meryeme Ayache, Ahmed Khoumsi, Mohammed Erradi   |            |
| <b>GIS Based Fuzzy Analytic Hierarchy Process for wind Energy Sites Selection.....</b>   | <b>168</b> |



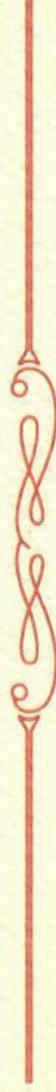
THE 2ND INTERNATIONAL CONFERENCE ON ADVANCED COMMUNICATION  
TECHNOLOGIES AND NETWORKING (COMMNET'19)  
APRIL 12-14, 2019, RABAT, MOROCCO

# CERTIFICATE OF PRESENTATION

WE HEREBY CERTIFY THAT

Evizal Abdul Kadir

*Islamic University of Riau, Indonesia*



HAS PRESENTED THE PAPER :

Smart Sensor Node of WSNs for River Water Pollution Monitoring System

**FAISSAL EL BOUANANI**  
COMMNET'19 GENERAL CHAIR



**PASCHALIS C. SOFOTASIOS**  
COMMNET'19 TPC CHAIR

# Network Traffic Monitoring and Analysis using Packet Sniffer

Apri Siswanto<sup>1</sup>, Abdul Syukur<sup>2</sup>, Evizal Abdul Kadir<sup>3</sup>, Suratin<sup>4</sup>  
<sup>1,2,3,4</sup>Department of Engineering, Faculty of Engineering  
Universitas Islam Riau, Indonesia

aprisiswanto@eng.uir.ac.id, abdulsyukur@eng.uir.ac.id, evizal@eng.uir.ac.id, suratin@student.uir.ac.id

**Abstract**—Traffic analysis using the internet is an activity to record data from user activities in using the Internet. This study aims to obtain data about the results of traffic in a graphical form so that it can find out the number of users who access the internet and use bandwidth. In this study, researchers also noted when the peak internet usage time in Telkom Vocational School Pekanbaru. The method used to get the results of the study is the packet sniffing method. Researchers can filter data packets from the http protocol application. Since user activity is more dominant in finding and downloading sites on the Internet. The tool used is Wireshark, this application is greatly helpful with features that are truly supportive and easy to analyze networks.

**Keywords**— Packet sniffer, Network Traffic, Monitoring, Internet, Wireshark

## I. INTRODUCTION

The usage of internet access in the Telkom Vocational High School, Pekanbaru, Indonesia is quite high. The use of the Internet has become a necessity for Telkom Vocational students due to student activities in learning activities using e-learning systems. For this reason, network monitoring and management of network traffic is a very important task in the field of computer networks [1]. This traffic analysis is used to monitor the traffic of internet access use, which is used by students and teachers of Telkom Vocational School, Pekanbaru to access websites, social media and others. In this case, only register users can access the Internet so that they can find out how much data bandwidth is used for internet needs at Telkom Vocational Schools. In this study, the authors conducted bandwidth measurements and network access monitoring in the Hypertext Transfer Protocol (HTTP) application so that the highest bandwidth usage traffic can be identified at a certain time..

To monitor and analyses data traffic, a packet sniffer tool is used. Packet sniffing is a technique of monitoring every packet that crosses the network. The tools commonly used to do packet sniffing techniques are generally Wireshark and Netcut. Packet sniffing is usually done by hackers or malicious intruders to carry out prohibited actions such as stealing passwords, and retrieving other important data. Then for the way the packet sniffing works is divided into three process, namely collecting, conversion, analysis, and data theft [2]. Nevertheless, in this study the sniffing packet was only used for monitoring and analysing network traffic..

## II. LITERATURE REVIEW

### A. Related Research

In this study to obtain optimal output research, literature review conducted related previous studies, so that it can be

used as a reference in research. There are several research studies that have been carried out by previous researchers, such as [1], they discussed packet analysis and network traffic monitoring over TCP protocol used Wireshark packet sniffer. The data analyzed are TCP time sequence graph, TCP Throughput graph, TCP round trip time graph. Based on data analysis of traffic on the network. The researchers proposed several recommendations for network traffic management. Similarly, [3] proposed a new method of monitoring systems. It can provide detailed information based on traffic behavior methods and a history of connected traffic. While comprehensive information on internet traffic used is monitored for analysis.

Qadeer, et al. [4] developed packet sniffer on the Linux platform for Intrusion Detection. The focus of this research is to analyze the bottleneck scenario that arises in the network. Then the next focus is to detect the presence of the software on the network and handle it in an efficient way. Lizarti, et al. [5] discuss traffic analysis in VPN using Simple Network Management Protocol (SNMP). In this study network traffic applications generate reports real-time traffic based on TCP ports and UDP and can be accessed privately with utilizing VPN technology so that it can help network administrators inside monitor and analyze problems that occur on the network.

### B. Network Monitoring

Monitoring an operational network can provide a network administrator with information to proactively manage the network and to report network usage statistics to others. Link activity, error rates, and link status are a few of the factors that help a network administrator determine the health and usage of a network. Collecting and reviewing this information over time enables a network administrator to see and project growth, and may enable the administrator to detect and replace a failing part before it completely fails. SNMP is commonly used to collect device information [6].

Simple Network Management Protocol (SNMP) was developed to allow administrators to manage nodes such as servers, workstations, routers, switches, and security appliances, on an IP network. It enables network administrators to monitor and manage network performance, find and solve network problems, and plan for network growth. SNMP is an application layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of three elements : SNMP manager, SNMP agents (managed node) and Management Information Base (MIB) [7].

### C. Packet Sniffing

Packet sniffing is tools that are used as monitoring data packet when a packet crosses a network. There are packet sniffing in the form of software, but there are also hardware-based devices that are installed directly along the network. Sniffer can handle data sent specifically to them. Sniffer can be used legally on the network by system administrators to monitor and solve traffic problems in their own networks. For example, if a computer has a communication problem with another computer, a administrators can view packet from one machine to another and determine the cause of the problem [8].

The packet sniffer consists of the following components [9]:

1. Hardware : standard network adapters .
2. Capture Filter : This is the most important part . It captures the network traffic from the wire, filters it for the particular traffic you want, then stores the data in a buffer.
3. Buffers : used to store the frames captured by the Capture Filter .
4. Real-time analyzer: a module in the packet sniffer program used for traffic analysis and to shift the traffic for intrusion detection.
5. Decoder : Protocol Analysis

Several examples of packet sniffing tools are wireshark kismet, tcpdump, cain and abel, ettercap, dsniiff, netstumbler, ntop, ngrep, etherape and kisMac. Wireshark is a network packet analyzer. A network packet analysis will try to capture network packets and try to display data packets as detailed as possible. User can think of network packet analysis as a measuring device used to check what happens inside a network cable, such as a voltmeter used by an electrician to check what is happening in an electrical cable. In the past, tools like the good were very expensive, exclusive or both. However, with the emergence of the wireshark all that has changed. Wireshark is one of the best open source analysis data packet available today [10].

### III. RESEARCH METHODOLOGY

The system development method used in this study is the Network Development Life Cycle (NDLC), which is a process approach in data communication that describes a cycle that has no beginning and end in observing the network. Like the following stages:

1. Analyze the need to conduct research, existing problems and analyze network topologies at Pekanbaru Telkom Vocational Schools.
2. Designing a network monitoring schedule on a specific time scale.
3. Conducts research execution (network monitoring), implementation of analysis and recording of the results of monitoring with capture.
4. Evaluation of result monitoring  
Management advice and conclusion see in Figure 1.

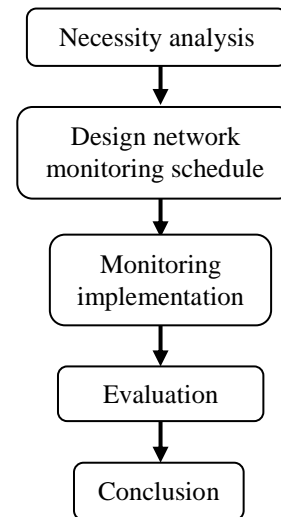


Fig 1. Research Method

#### A. Network Topology in Telkom Vocational school, Pekanbaru, Indonesia

The Internet network system used at the Pekanbaru Telkom Vocational School is a telkom network that is optical fiber from an ISP center in the School Laboratories and then subdivided by using access control on the proxy, then directed to the switches and access points of each Laboratory in Schools. The Internet network in Lab also uses a login access system by using a server as a tool to filter data on students and school teachers, to find out the increasing number of data access and Internet needs of students researchers analyze the Internet usage traffic at Telkom Vocational Schools, Pekanbaru, Indonesia. For more details see figure 2.

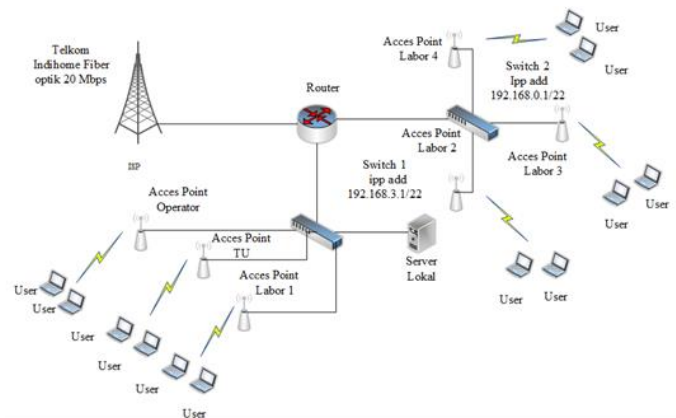


Fig. 2. Network topology in Telkom vocational school

The design of the monitoring scheme that will be carried out in the study uses port lines on routers that are connected to the Internet Service Provider (ISP) provided by Telkom with a bandwidth of 20 Mbps. The router port will be connected to the Personal Computer (PC) monitoring in order to analyze internet usage traffic at telkom Vocational School. The tools used, will be installed on the PC monitoring tools that are used, namely wireshark. Figure 3 shows the monitoring system scheme.



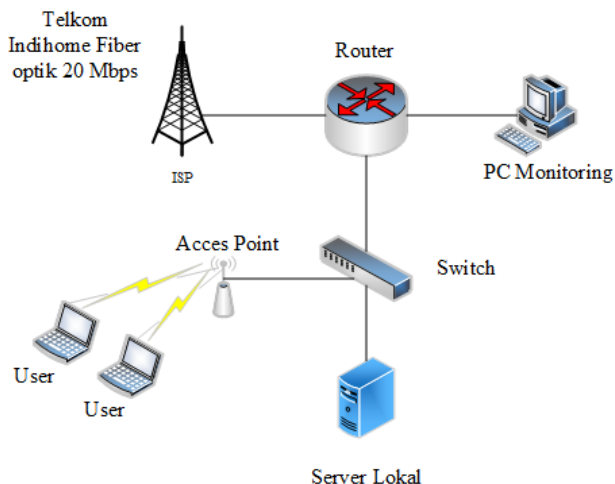


Fig. 3. Monitoring system scheme

To facilitate monitoring at Telkom Vocational Network, user must know the IP address of Switch 1 and Switch 2, see table 3.1

Table 1. IP Address monitoring

| Switch 1            | IP Address                        |
|---------------------|-----------------------------------|
| Lab 1               | -                                 |
| Administration Room | -                                 |
| Operator Room       | 192.168.3.1/22                    |
| Switch 2            | IP address                        |
| Lab 2               | -                                 |
| Lab 3               | -                                 |
| Lab 4               | 192.168.0.1/22                    |
| Network Hardware    | 192.168.3.1/22-<br>192.168.0.1/22 |

#### IV. RESULT AND DISCUSSION

In the process of building an optimum network, the results of analyzing Internet usage by the user are very much needed. Because the data analysis results can be used to evaluate the design of a network system that is more optimal in managing bandwidth for user requirements. In this research, the researcher analyses Internet usage traffic by using wireshark. These tools used to sniff on routers and proxy to get packets from a network and filter HTTP packet data.

In this study, researchers conducted a study to analyse the Internet traffic usage in Telkom vocational during two weeks or fourteen days. The results of this study are in the form of traffic from bandwidth usage by users in school. The results of the graph displayed are only the first day, the eighth and the last day. First day's researches were conducted on Monday, October 8, 2018, the highest access time at 10:33 WIB and the bandwidth size accessed by users were 25966 bytes / second, and the average bandwidth speed accessed 637 bytes / second and total bandwidth usage / day 3563328 Bytes (see figure 4)

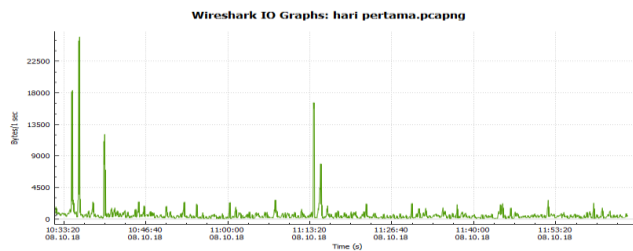


Fig. 4 Result graph of monitoring in first day

Then, the results of the data traffic analysis on the 8th day are carried out on Monday, October 15, 2018, the highest access time is at 10:10 WIB and the bandwidth size accessed by users is 67480 Bytes / second, the average bandwidth speed is accessed 13k Bytes / second and total bandwidth usage / day 138400867 Bytes. See in figure 5.

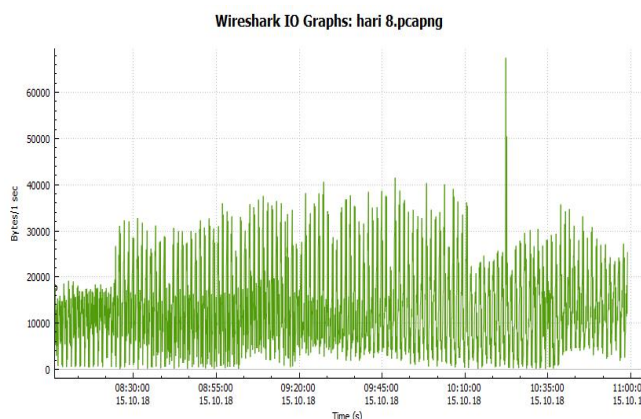


Fig. 5. The result graph of monitoring 8<sup>th</sup> day

After that, the results of traffic analysis data on day 14 are carried out on Sunday 21 October 2018, the highest access time is at 11:26 WIB and the bandwidth size accessed by users is 35128 Bytes / second, the average bandwidth speed accessed is 2630 Bytes / second and total bandwidth usage / day 62262684 Bytes. See picture 6.

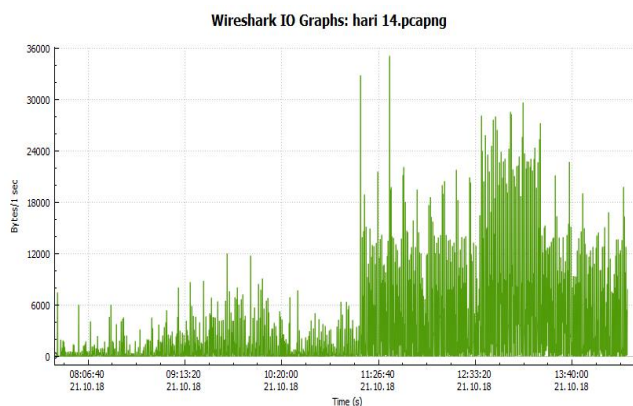


Fig. 6. The result graph of monitoring last day

Based on the results of analysis of internet usage traffic in Telkom vocational school, Pekanbaru for two weeks can be summarized such as data in table 1.

Table .1 Traffic Analysis Results.

| Date       | Bandwidth highest access (bps) | Bandwidth average (bps) | Total bandwidth access (bps) | The number of IP Address user |
|------------|--------------------------------|-------------------------|------------------------------|-------------------------------|
| 8/10/2018  | 25966                          | 5100                    | 3563328                      | 77                            |
| 9/10/2018  | 540483                         | 65536                   | 77.323.912                   | 466                           |
| 10/10/2018 | 207313                         | 235520                  | 52566146                     | 141                           |
| 11/10/2018 | 3302                           | 3472                    | 561909                       | 52                            |
| 12/10/2018 | 57051                          | 107520                  | 27986432                     | 91                            |
| 13/10/2018 | 119220                         | 91136                   | 94346555                     | 99                            |
| 14/10/2018 | 10808                          | 5870                    | 2744025                      | 38                            |
| 15/10/2018 | 67480                          | 108544                  | 138400867                    | 108                           |
| 16/10/2018 | 967436                         | 236544                  | 51192592                     | 122                           |
| 17/10/2018 | 882388                         | 88064                   | 143385889                    | 135                           |
| 18/10/2018 | 42669                          | 59392                   | 95546745                     | 131                           |
| 19/10/2018 | 304971                         | 48128                   | 42837893                     | 82                            |
| 20/10/2018 | 45108                          | 6611                    | 11366544                     | 90                            |
| 21/10/2018 | 35128                          | 21504                   | 62262684                     | 119                           |
| Average    |                                | 13 Mbps                 |                              | 125                           |

The results of the average bandwidth for fourteen days is 13 / Mbps .The list of user ip recorded when accessing the highest and lowest bandwidth is as follows:

1. List of IP users recorded accessing the internet on the school network on October 9, 2018 the number of IPs is 466 users.
2. List of IP users recorded accessing the internet on the school network on October 14, 2018 the number of IPs is 38 users.

#### V. CONCLUSION

Based on the data obtained, the average bandwidth usage per second is 13 Mbps from an average of 125 users. This means that there are still 7 Mbps spaces that are not used by the user. Nevertheless, if you assume the number of users is 500 users, then the average user gets 40 Kbps, allowing for convenient the Internet browsing access. If for users to access information systems or cloud-based systems, the user needs at least 200 Kbps. While the user for video streaming needs 300 Kbps. Thus, based on the analysis of current traffic data, 20 Mbps is still sufficient for Telkom Vocational school needs, Pekanbaru, although ideally if there are 500 users with medium users, it is better to use 100 Mbps internet bandwidth packages.

#### REFERENCES

- [1] A. Bhandari, S. Gautam, T. K. Koirala, and M. R. Islam, "Packet Sniffing and Network Traffic Analysis Using TCP—A New Approach," in *Advances in Electronics, Communication and Computing*, ed: Springer, 2018, pp. 273-280.
- [2] S. Ansari, S. Rajeev, and H. Chandrashekar, "Packet sniffing: a brief introduction," *IEEE potentials*, vol. 21, pp. 17-19, 2002.
- [3] S. L. Rosa and E. A. Kadir, "Abnormal internet usage detection in LAN Islamic University of Riau Indonesia," in *Proceedings of the International Conference on Intelligent Science and Technology*, 2018, pp. 17-22.
- [4] M. A. Qadeer, A. Iqbal, M. Zahid, and M. R. Siddiqui, "Network traffic analysis and intrusion detection using packet sniffer," in *Communication Software and Networks, 2010. ICCSN'10. Second International Conference on*, 2010, pp. 313-317.
- [5] N. Lizarti and W. Agustin, "Aplikasi Network Traffic Monitoring Menggunakan Simple Network Management Protocol (SNMP) pada Jaringan Virtual Private Network (VPN)," *SATIN-Sains dan Teknologi Informasi*, vol. 1, pp. 27-34, 2015.
- [6] T. Lammle, *CCNA Routing and Switching Study Guide: Exams 100-101, 200-101, and 200-120*: John Wiley & Sons, 2013.
- [7] T. Lammle, *CCNA Cisco Certified Network Associate Deluxe Study Guide*: John Wiley & Sons, 2011.
- [8] T. King, "Packet sniffing in a switched environment," *SANS Institute, GESC practical*, vol. 1, 2002.
- [9] P. Asrodia and H. Patel, "Analysis of various packet sniffing tools for network monitoring and analysis," *International Journal of Electrical, Electronics and Computer Engineering*, vol. 1, pp. 55-58, 2012.
- [10] L. Chappell and G. Combs, *Wireshark network analysis: the official Wireshark certified network analyst study guide*: Protocol Analysis Institute, Chappell University, 2010.