IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1994

Pendeteksian Anomali Penggunaan Internet di LAN Universitas Islam Riau Indonesia

Sri Listia Rosa[1]
[1]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Islam Riau
Jl. Kaharuddin Nasution No. 113 Marpoyan, Pekanbaru, Riau, Indonesia 28284
e-mail: srilistiarosa@eng.uir.ac.id

Abstract

Increasing internet network traffic in a Local Area Network (LAN) will impact to internet access performance. Abnormal internet traffic monitoring system is very important to detect anomaly usage of internet bandwidth. In Islamic University of Riau (UIR) one of the issue related internet usage and normal method is by tapping a monitoring computer to the main terminal of LAN or source of internet provider. This research proposes a new method of monitoring system that gives detail information by using traffic behavior method and history of traffic connected, whereas detail information of internet bandwidth used is monitored for analysis. In this research case location is in Islamic University of Riau, Indonesia campus LAN area. Results shows graph of monitoring in day time because of student activities only in that time, various website and link access by students and staff in the campus be able to captured including duration with specific time. This method gives continues and accurate data to capture anomaly data use including Internet Protocol (IP) address of computer or device connected. The system help operator to give report related to internet usage and user who connected as well as data used in automatic system.

Keywords: *Internet Usage; Detection; LAN; UIR*

Abstrak

Meningkatnya lalu lintas jaringan internet di Local Area Network (LAN) akan berdampak pada kinerja akses internet. Sistem pemantauan ketidaknormalan lalu lintas internet sangat penting untuk mendeteksi penggunaan bandwidth internet secara tidak normal. Di Universitas Islam Riau (UIR) salah satu isu terkait penggunaan internet dan metode yan biasa digunakan adalah dengan memeriksa komputer melalui pemantau ke terminal utama LAN atau sumber penyedia internet. Penelitian ini menggunakan metode baru untuk sistem pemantauan yang memberikan informasi detail dengan menggunakan metode pemantauan jaringan dari berbagai perilaku dan riwayat trafik yang terhubung ke internet, sedangkan informasi detail bandwidth internet yang digunakan di pantau untuk di analisa. Lokasi penelitian dilakukan di kawasan LAN yang berada di Universitas Islam Riau, di area LAN kampus. Hasil analisa menunjukkan grafik pemantauan pada siang hari lebih besar karena kegiatan siswa hanya pada waktu itu, berbagai situs web yang di akses dan tautan lainnya oleh mahasiswa dan pegawai di lingkungan kampus dapat dideteksi termasuk durasi yang digunakan serta dengan waktu tertentu. Metode ini memberikan data yang terus menerus dan sangat akurat untuk menangkap penggunaan data yang tidak normal termasuk alamat Internet Protocol (IP) komputer atau perangkat yang terhubung ke internet. Sistem ini membantu operator untuk memberikan laporan terkait penggunaan internet dan pengguna yang terhubung serta data yang digunakan secara otomatis tanpa perlu di lakukan secara manual.

Kata kunci: Pemakaian Internet, Deteksi, LAN, UIR

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1994

1. PENDAHULUAN

Peningkatan penggunaan internet yang sangat pesat saat ini menyebabkan permintaan akan mutu layanan yang baik harus ditingkatkan, tidak hanya bisa terhubung dengan internet. Beberapa penelitian yang terkait dengan penelitian yang penulis angkat seperti, Roland (2013), pada penelitian ini membahas tentang analisis kinerja trafik web browser melalui software wireshark, dengan tujuan untuk mengetahui kinerja trafik di dalam jaringan internet melalui web browser. Web browser atau disebut penjelajah web, adalah perangkat lunak yang berfungsi menampilkan dan melakukan interaksi dengan dokumen-dokumen yang disediakan oleh server web. Perbedaan pada penelitian ini adalah peneliti menggunakan software wireshark untuk menganalisa penggunaan bandwith dengan parameter waktu tertentu sehingga dapat mengetahui kapan waktu puncak pengaksesan bandwidth paling besar.

Di dalam [1][2], penelitian ini membahas tentang analisa trafik menggunakan Multi Router Traffic Grapher (MRTG) berbasis Simple Network Management Protocol (SNMP). Pada penelitian ini analisa trafik yang dilakukan adalah menganalisa bandwidth yang digunakan pada saat mengakses server. Karena jalur utama pengaksesan terdapat di server, setiap user sebelum mengakses harus mengisi form login. Monitoring bandwidth pada penelitian ini berdasarkan waktu yang sudah ditentukan perhari, perbulan dan pertahun. Pebedaan pada penelitian ini adalah peneliti menggunakan tools Wireshark selain itu peneliti melakukan penelitian langsung ke pusat data melalui ports router sedangkan penelitian di atas hanya menganalisa trafik langsung ke Domain Name Server (DNS) server website.

Penelitian ini [3][4] membahas monitoring bandwidth dengan cara mengkelompokan client dan server sehingga mudah untuk mengetahui penggunaan bandwidth yang digunakan oleh user. Perbedan pada penelitian ini dengan penulis, penelitian ini hanya monitoring kesetabilan pada jaringan dan membagi akses pada user sedangkan penulis monitoring waktu puncak pengaksesan bandwidth dengan mengukur akses ke jalur Hypertext Transfer Protocol (HTTP) dan aplikasi yang digunakan adalah Wireshark.

Pada penelitian ini bertujuan untuk menganalisa sebuah jaringan terstruktur di UIR dengan memahami materi yang dibutuhkan untuk penelitian ini lebih lanjut. Adapun beberapa materi yang akan dipahami sebelum melanjutkan penelitian ini adalah teori menggenai trafik, bandwith, Transport Control Protocol/Internet Protocol (TCP/IP), Open System Interconnection (OSI), simple network management protocol (SNMP) Protokol jaringan, dan aplikasi yang mendukung seperti wireshark [5][6].

2. PENGEMBANGAN JARINGAN INTERNET LIFE CYCLE

Traffict monitoring adalah sebuah metode yang lebih canggih dari networking monitoring. Metode ini melihat paket actual dari traffic pada jaringan dan menghasilkan laporan berdasarkan traffic jaringan. Pada hal ini tidak hanya mendeteksi peralatan yang gagal, tetapi berfungsi untuk menentukan apakah suatu komponen overload atau terkonfigurasi secara buruk. Kelemahannya adalah karena biasanya bekerja pada suatu segmen tunggal pada satu waktu jika data perlu didapat dari segmen lain, software monitoring harus bergerak pada segmen tersebut, tapi hal ini dapat diatasi dengan menggunakan agent pada segmen remote network [7].

IT Journal Research and Development
Vol.2, No.2, Maret 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1994

Metode pengembangan sistem yang digunakan dalam penelitian ini adalah Network Development Life Cycle (NDLC), yaitu suatu pendekatan proses dalam komunikasi data yang menggambarkan siklus yang tiada awal dan akhir dalam mengamati jaringan. Seperti tahap berikut:

1. Menganalisis kebutuhan untuk melakukan penelitian, permasalahan yang ada, topologi jaringan di UIR.
2. Merancang jadwal monitoring jaringan dalam skala waktu tertentu.
3. Simulasi prototype melakukan eksekusi penelitian (monitoring jaringan).
4. Implementasi analisis dan perekaman hasil monitoring dengan di capture.
5. Manajemen, pengelolaan alokasi bandwidth jaringan yang dilakukan administrator.
6. Lokasi penelitian adalah jaringan leased line UIR

2.1 Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) adalah Internet Protocol Suite, yang dibuat oleh Internet Engineering Task Force (IETF) pada tahun 1988. Tujuan awal diciptakannya protokol SNMP dalam mengatur berbagai device yang semakin banyak seiring dengan berkembangnya jaringan internet. SNMP dikembangkan untuk menyediakan peralatan manajemen jaringan yang mendasar dan mudah diimplementasikan untuk rangkaian protokol Transmission Control Protocol/Internet Protocol (TCP/IP). SNPM merupakan protokol dari lapis Application yang digunakan untuk network management system, melakukan monitoring perangkat jaringan sehingga lebih mudah dalam memberi informasi bagi pengelola jaringan [8].

Server manajemen SNMP dapat melakukan test untuk memeriksa status antar perangkat jaringan yang terhubung secara fisik. Pada lapis data link, server manajemen SNMP digunakan untuk mengkonfigurasi, menaktifkan, dan mematikan koneksi di jaringan. Server manajemen SNMP dapat menerima frame data keluar dan masuk jaringan, dan mengetahui error pada setiap perangkat yang sedang berkomunikasi. Pada lapisan network, server manajemen SNMP memeriksa IP address assigments, address translation tables, dan routing tables. Di lapisan transport, server manajemen SNMP dapat menghitung durasi koneksi perangkat dengan TCP, sehingga server manajemen SNMP mampu menghitung Traffic TCP dan User Datagram Protocol (UDP) serta menghitung error yang terjadi. Dengan demikian SNMP dapat digunakan untuk pengawasan, pengkoleksian statistik, pemeriksa untuk kerja dan keamanan dari suatu jaringan. Untuk melakukan fungsi-fungsi tersebut SNMP dibagi menjadi tiga bagian yang saling berkerja sama satu dengan lainnya yaitu: Managed Device, Agent, dan Network Management System.

2.2 Wireshark

Wireshark adalah penganalisa paket jaringan. Sebuah analisa paket jaringan akan mencoba untuk menangkap paket jaringan dan mencoba untuk menampilkan data paket serinci mungkin. Anda bisa memikirkan analisa paket jaringan sebagai alat pengukur yang digunakan untuk memeriksa apa yang terjadi di dalam kabel jaringan, seperti voltmeter digunakan oleh seorang teknisi listrik untuk memeriksa apa yang terjadi dalam sebuah kabel listrik (tetapi pada tingkat yang lebih tinggi, tentu saja). Di masa lalu, alat-alat seperti yang baik sangat mahal, eksklusif atau keduanya. Namun dengan munculnya wireshark semua itu telah berubah. Wireshark adalah salah satu yang terbaik open source analisa paket yang tersedia saat ini [9].

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1994

Berikut adalah beberapa contoh orang menggunakan Wireshark untuk:

1. Administrator jaringan menggunakannya untuk memecahkan masalah jaringan
2. insinyur keamanan jaringan menggunakannya untuk memeriksa masalah keamanan
3. Pengembang menggunakannya untuk implementasi protokol men-debug
4. Orang-orang menggunakannya untuk belajar internal protokol jaringan

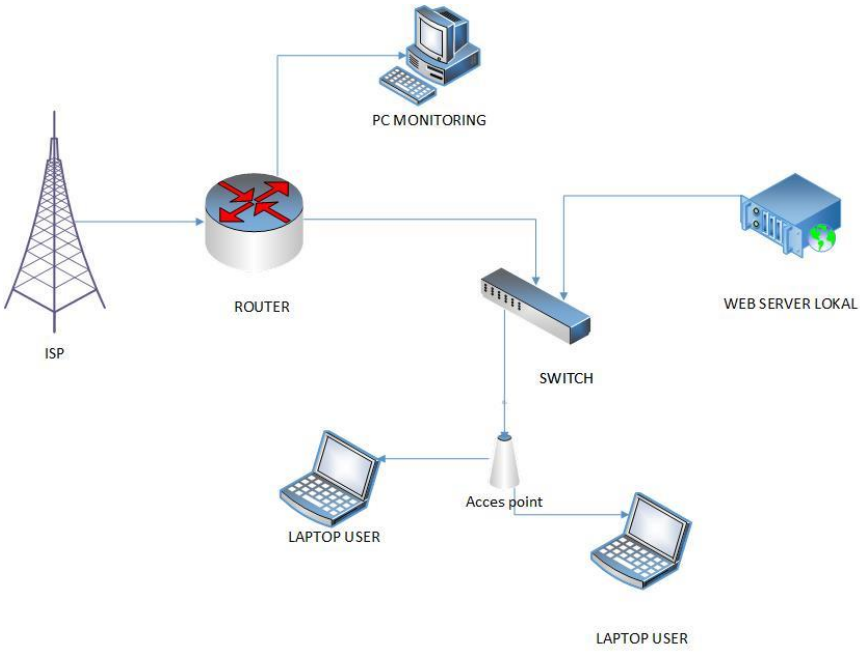
Disamping contoh-contoh ini wireshark dapat membantu dalam banyak situasi lain juga. Berikut ini adalah beberapa dari banyak fitur Wireshark tersedia [10].

1. Tersedia untuk UNIX dan Windows.
2. Tangkap hidup paket data dari antarmuka jaringan.
3. Buka file yang berisi data paket yang diambil dengan tcpdump / WinDump, Wireshark, dan sejumlah program capture paket lainnya.
4. Impor paket dari file teks yang berisi tempat pembuangan hex dari paket data.
5. Tampilan paket dengan informasi protokol yang sangat rinci.
6. Simpan data paket yang diambil.
7. Ekspor beberapa atau semua paket di sejumlah format capture file yang.
8. Filter paket pada banyak kriteria.
9. Cari untuk paket pada banyak kriteria.
10. Layar Colorize paket berdasarkan filter.
11. Buat berbagai statistik

3. PENGEMBANGAN JARINGAN INTERNET LIFE CYCLE

Sistem jaringan internet yang digunakan di UIR adalah Point to Point yang mana jaringan internet dari sebuah pusat ISP di BAIT UIR dan kemudian dibagi lagi dengan menggunakan access control pada mikrotik, selanjutnya diarahkan ke switch dan access point setiap Fakultas di UIR. Jaringan internet di BAIT juga menggunakan sistem akses login dengan menggunakan server local sebagai alat bantu untuk melakukan fiter data mahasiswa yang menggunakan akses internet adalah mahasiswa UIR, karena menu akses login mengunakan data Nomor Pokok Mahasiswa (NPM) setiap mahasiswa di UIR. Untuk menggetahui jumlah data akses dan kebutuhan internet mahasiswa yang terus meningkat peneliti melakukan analisa trafik penggunaan internet di UIR.

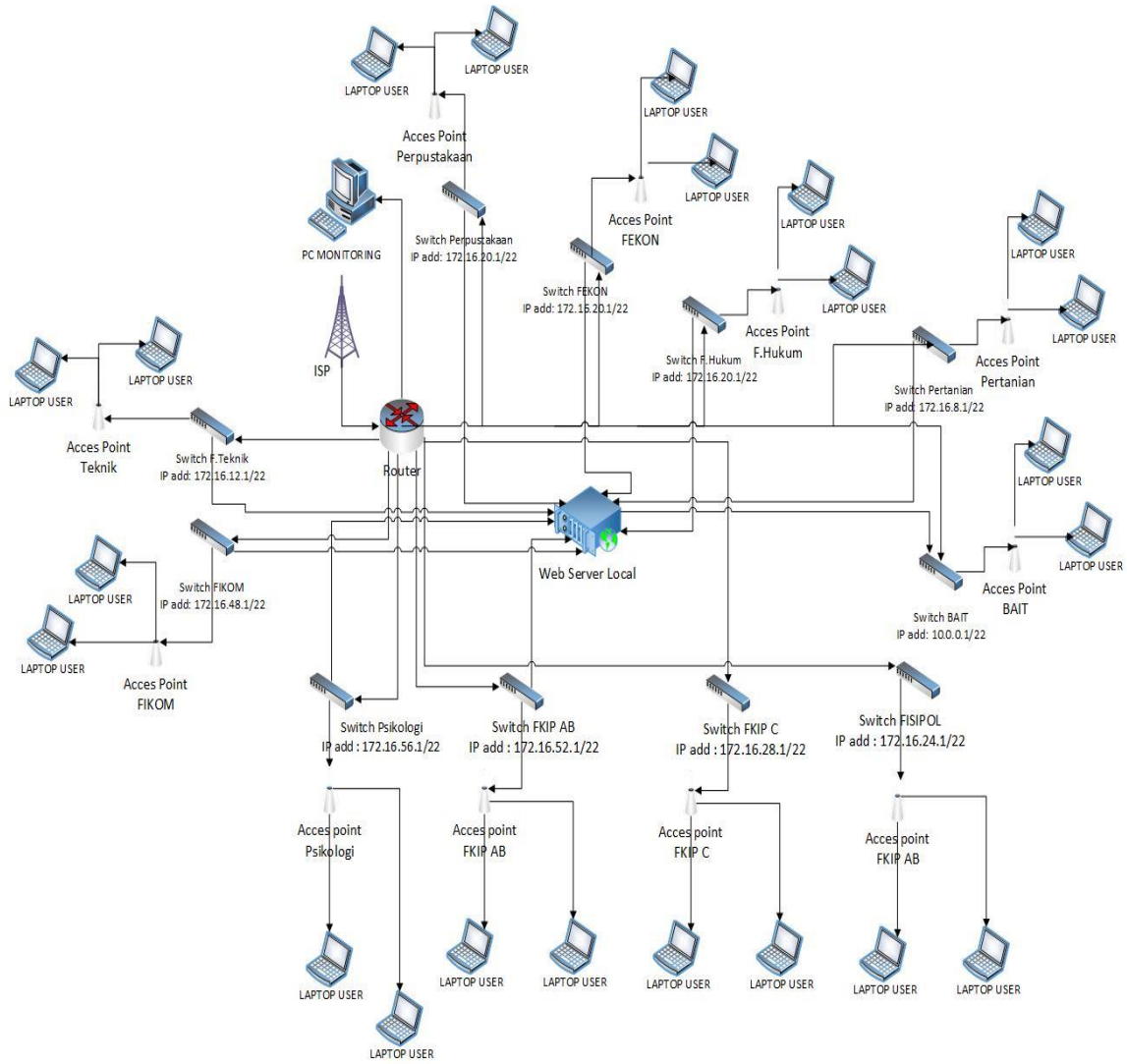
IT Journal Research and Development
Vol.2, No.2, Maret 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1994



Gambar 1. Skema Diagram Pemantauan Data Anomali Penggunaan Internet.

Pada gambar 1 adalah perancangan skema monitoring yang akan dilakukan pada penelitian ini. Peneliti akan menggunakan jalur port pada router yang terhubung dengan Internet Service Provider (ISP). Pada port router akan dihubungkan ke Personal Computer (PC) monitoring agar dapat menganalisa trafik penggunaan internet di UIR. Adapun tools yang digunakan akan di install pada PC monitoring tools yang digunakan yaitu wireshark. Untuk melihat topologi detail dari stuktur jaringan UIR berserta masing-masing IP di setiap Fakultas di UIR, seperti pada gambar 2.

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1994



Gambar 2. Diagram Lengkap Sistem Pemanatauan Data Anomali Penggunaan Internet.

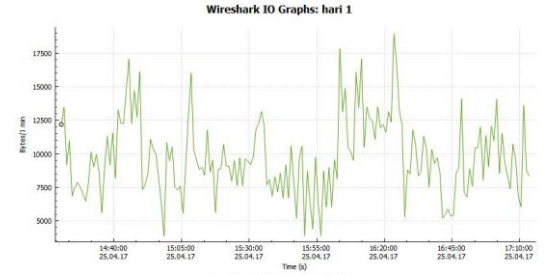
Sniffing merupakan proses analisa paket data pada sistem jaringan komputer, yang diantaranya dapat melakukan monitoring dan menangkap semua trafik jaringan yang terhubung tanpa peduli kepada siapa paket itu dikirimkan [11]. Untuk menganalisa paket-paket data yang melintas pada jaringan internet serta mengukur sudah optimal atau tidaknya penggunaan jaringan internet dan dapat mengetahui waktu puncak pengaksesan internet tertinggi dengan melakukan sniffing.

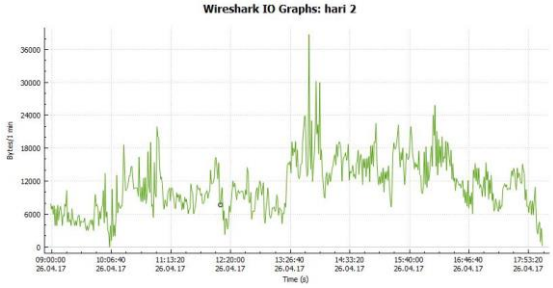
4. HASIL DAN PEMBAHASAN

Dalam proses membangun sebuah jaringan yang optimal sangat dibutuhkan hasil analisa trafik penggunaan internet oleh user karena dengan adanya data hasil analisa dapat digunakan untuk melakukan evaluasi perancangan sebuah sistem jaringan yang lebih optimal lagi dalam melakukan manajemen bandwith untuk kebutuhan pengguna. Pada skripsi ini peneliti melakukan analisa trafik penggunaan internet dengan menggunakan tools wireshark untuk melakukan sniffing pada router dan mikrotik untuk

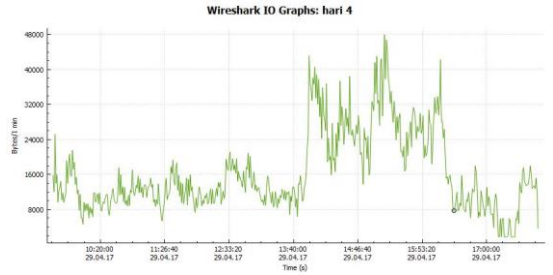
IT Journal Research and Development
Vol.2, No.2, Maret 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1994

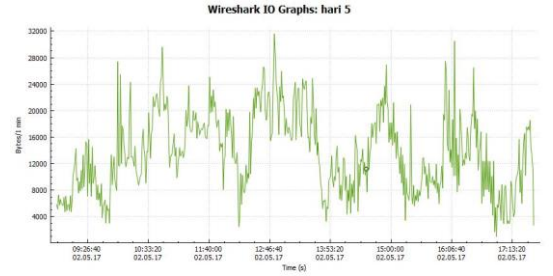
mendapatkan paket dari sebuah jaringan dan melakukan filter data-data paket yang berjenis HTTP karena data jenis. Gambar 3 menunjukkan grafik penggunaan internet dan pemantauannya setiap hari.





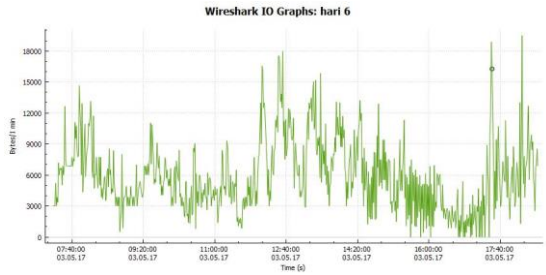
(a) (b)

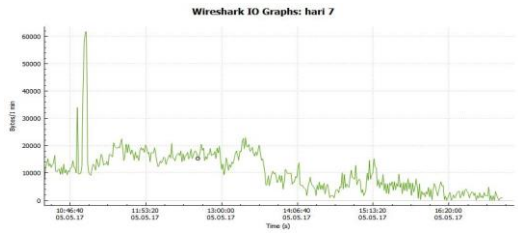




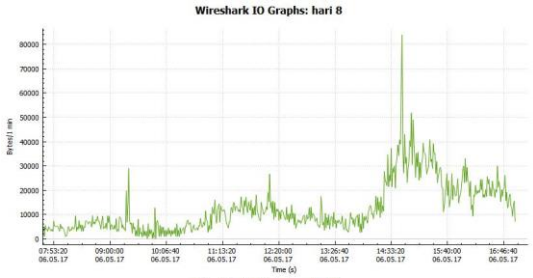
(c) (d)

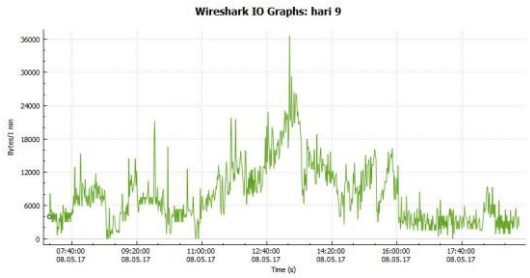
IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1994





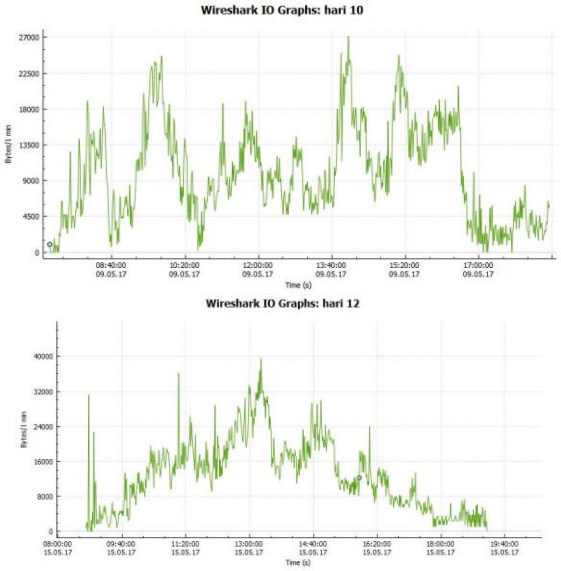
(e) (f)





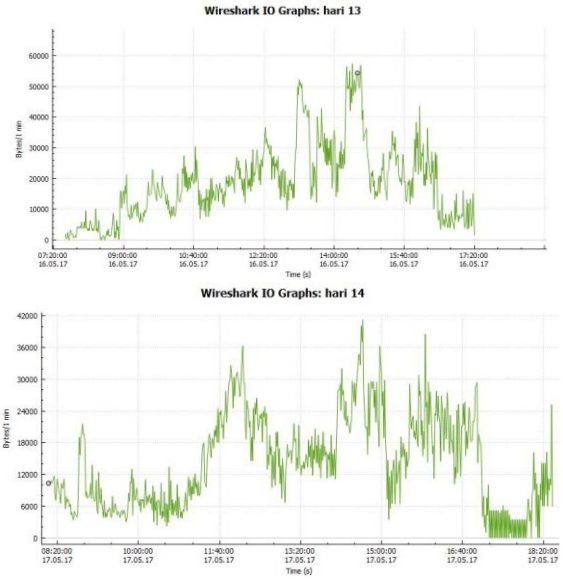
(g) (h)

IT Journal Research and Development
Vol.2, No.2, Maret 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1994



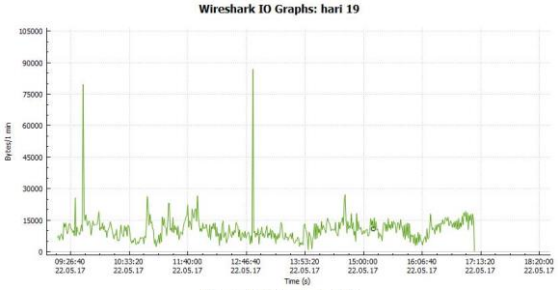
(i) (j)

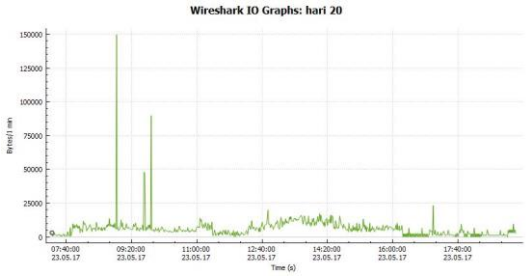
Gambar 3. Pendeteksian anomali penggunaan internet hari (a) hari pertama – (j) hari ke sepuluh



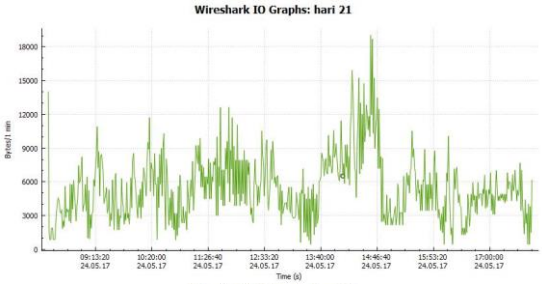
(a) (b)

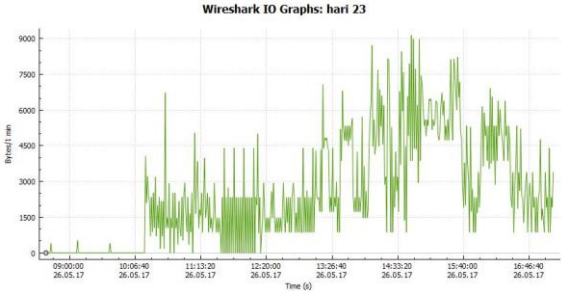
IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1994





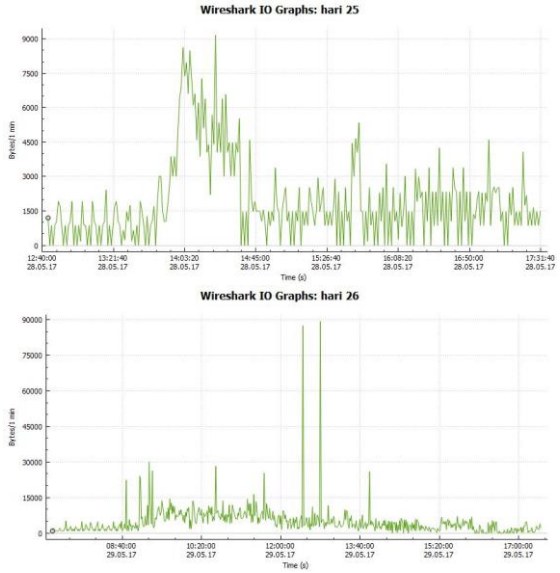
(c) (d)





(e) (f)

IT Journal Research and Development
Vol.2, No.2, Maret 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1994



(g) (h)

Gambar 4. Pendeteksian anomali penggunaan internet hari (a) hari kesebelas dan hingga (h) hari ke delapanbelas

Berdasarkan pemantauan selama delapan belas hari seperti yang ditunjukkan pada grafik pada gambar 4, hasil deteksi umumnya penggunaan internet sangat aktif dan bervariasi pada siang hari terutama pada jam aktif kantor yaitu dari pukul 08.00 hingga pukul 16.00. Grafik menunjukkan beberapa hari peningkatan penggunaan sangat drastik dan kembali normal setelah beberapa selang waktu, beberapa grafik menunjukkan juga data tiba-tiba naik secara drastis dan kembali normal hanya dalam selang beberap menit.

5. KESIMPULAN

Penelitian ini berlangsung di kampus Universitas Islam Riau, akses internet sangat penting bagi mahasiswa dan dosen. Berdasarkan penelitian dan analisis dalam deteksi abnormal penggunaan internet seperti yang ditunjukkan dalam hasil, beberapa grafik meningkat penggunaan data secara luar biasa dan turun secara tiba-tiba, hasil lainnya menunjukkan terus meningkat tetapi mempertahankan yang membuat akses internet sangat lambat dan berdampak pada operasional Universitas. Sistem pendeteksian abnormal menemukan pengguna yang serupa untuk mengakses internet dengan situs web serupa pula untuk mengakses dan menautkannya, beberapa penggunaan yaitu live streaming dan konferensi video. Sebagai hasil yang ditunjukkan dapat disimpulkan bahwa pembatasan bandwidth internet merupakan solusi utama untuk masalah kampus yang saat ini terjadi tetapi didukung dengan manajemen bandwidth terhadap pengguna yang merupakan solusi yang sangat membantu kemudian diikuti oleh peningkatan langganan bandwidth dari provider.

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1994

DAFTAR PUSTAKA

[1] H. James Baxter., 2014, Wireshark Essentials, Packt Publishing.
[2] Ferdy M. Adriant dan Mardianto Is., 2015, Implementasi Wireshark Untuk Penyadapan (Sniffing) Paket Data Jaringan, Jurnal Teknik Informatika ISSN: 2460-8696.
[3] Kurniawan Edy dan Khoirurrosyidin., 2015, Analisa Penggunaan Bandwidth Untuk Optimalisasi Pemanfaatan Internet dan Internet di Jaringan Universitas, *Jurnal SANTEK* ISBN 978-602-14355-0-5.
[4] Kurniawan A., 2012, *Network Forensic*. Yogyakarta: Andi Offsite.
[5] Oktavianus Roland Lukas Sihombing dan Zulfin Muhammad., 2013, Analisis Kinerja Trafik Web Browser Dengan Wireshark Network Protocol Analyzer Pada Sistem Client-Server, *Jurnal Fakultas Teknik Universitas Sumatera Utara (USU)* Vol. 02, No. 03, 2013, hal 1-6.
[6] Orzach Yoram., 2013, *Network Analysis Using Wireshark Cookbook*, Packt Publishing.
[7] Sanders Chris., 2011, *Practical Packet Analysis Using Wireshark To Solve Real-World Network Problems*, No Starch Press.
[8] Parmo I., 2008, Mengenal Dunia Hacking : Sniffing. Retrieved From isparmo.web.id: http://isparmo.web.id/2008/06/06/mengenal-dunia-hacking-sniffing/
[9] Sharpe Richard., Warnicke Ed., 2014, *Wireshark User's Guide: For Wireshark 2.1*, Ulf Lamping.
[10] Singh A., 2013, *Wireshark Starter*, Birmingham: Packt Publishing
[11] Arta, Y. (2017). Implementasi Intrusion Detection System Pada Rule Based System Menggunakan Sniffer Mode Pada Jaringan Lokal. *IT Journal Research And Development*, *2*(1), 43 - 50. vol2(1).