Jurnal Artificial, Vol 1 No 1, April 2023

Implementasi Keamanan Jaringan Komputer dengan Menggunakan Model Forensik pada SMKN 1 Palopo

Sri Angraeni [1], Alim Surya Saruman [2*]

[1, 2] Universitas Cokroaminoto Palopo

* alimsurya@uncp.ac.id

Abstrak

Penelitian bertujuan untuk mengimplementasikan keamanan jaringan menggunakan model forensik pada jaringan sekolah dimana terdapat masalah koneksi jaringan yang lambat karena adanya pengguna yang membobol jaringan *wireless* dari luar sekolah. Penelitian ini dilaksanakan di SMK Negeri 1 Palopo. Metode penelitian yang digunakan dalam penelitian ini adalah kualitatif. Metode pengumpulan data yang terdiri dari metode observasi dimana peneliti mengunjungi lokasi penelitian pada Negeri 1 Palopo dan meninjau langsung keadaan, wawancara kepada staf dengan cara menghubungi kepala laboratorium komputer sekolah yang ada di SMK Negeri 1 Palopo. Hasil dari penelitan adalah dengan menggunakan menggunakan Model Proses Forensik dapat mengimplementasikan keamanan jaringan pada serangan DDOS menggunakan *software* LOIC, data analisis tersebut bisa dijadikan salah satu pembuktian terjadinya serangan, selain itu bisa digunakan sebagai bahan untuk pelaporan kepada pihak berwajib (jika diperlukan). Dari hasil serangan dapat dilakukan analisis, yaitu pukul berapa terjadi serangan, jenis serangan, serta total packet.

Kata Kunci: *Model forensik, DDOS,* LOIC, *Jaringan Komputer, Sistem Keamanan*

Pendahuluan

Pada saat ini isu keamanan jaringan sangat penting dan perlu mendapat perhatian. Jaringan yang terhubung ke Internet secara inheren tidak aman dan selalu dapat dieksploitasi oleh peretas di jaringan LAN kabel dan nirkabel. Ketika data dikirim, ia melewati beberapa terminal untuk mencapai tujuan. Dengan kata lain, memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menguping atau memodifikasi data. Sebuah sistem keamanan jaringan yang terhubung ke Internet perlu direncanakan dan dipahami dengan baik dalam pengembangan desainnya agar dapat secara efektif melindungi sumber daya pada jaringan dan meminimalkan serangan peretas. (Nugroho, 2012).

Teknologi informasi terus berkembang karena memiliki dampak yang lebih besar pada cara kita menikmati pekerjaan, komunikasi, belanja, dan hiburan daripada sebelumnya. Program keamanan komputer online mencakup dua bidang utama. Salah satunya adalah keamanan jaringan, yang mencakup perlindungan jaringan TI dari peretas, kehilangan data, pencurian identitas, virus, dan jenis serangan malware lainnya. Forensik komputer ini termasuk investigasi kejahatan dunia maya seperti: pencurian informasi pribadi, penyalahgunaan aset pihak ketiga, pornografi di bawah umur, pengawasan internet.

Secara khusus dan mendalam masalah proses pengungkapan bukti, mengumpulkan dan menganalisis bukti digital dari berbagai sumber seperti hard drive komputer dan email, dan menyiapkan bukti untuk penuntutan kejahatan komputer.

Dunia komunikasi data global dan perkembangan teknologi informasi dan perangkat lunak yang selalu berubah, keamanan merupakan isu krusial, termasuk keamanan fisik, keamanan data, dan keamanan aplikasi. Perlu kita sadari bahwa sangat mustahil untuk mencapai keamanan seperti yang terjadi di dunia nyata saat ini. Di luar keamanan sistem komputer, ada lebih dari satu area yang sepenuhnya aman di mana penjaga keamanan berada, tetapi yang dapat kami lakukan adalah mengurangi gangguan keamanan. (Sulianta, 2016). Kejahatan-kejahatan tersebut dapat dicegah dengan menggunakan metode peristiwa karena model proses forensik adalah aktivitas yang mengumpulkan, mencatat, dan menganalisis peristiwa dalam jaringan untuk menemukan penyebab serangan keamanan dan masalah lainnya. Kinerja forensik terletak pada pengumpulan dan analisis data dari berbagai sumber daya komputer, termasuk log antivirus, log database, dan log dari aplikasi yang digunakan. Sistem deteksi intrusi dapat menggunakan sistem deteksi intrusi**.** Snort adalah IDS berbasis open source. Model proses forensik menggunakan Snort untuk menganalisis semua lalu lintas jaringan dan mencegat dan mencari jenis intrusi jaringan. (Singh, 2009)

Sekolah Menengah Kejuruan Negeri (SMKN) 1 Palopo, merupakan salah satu sekolah yang di Kota Palopo memiliki jaringan internet yang luas dimana jaringan internet tersebut rentan terhadap serangan jaringan, karena jaringan sekolah belum menerapkan sebuah sistem keamanan jaringan. Maka dari itu jaringan di SMKN 1 Palopo sering di retas oleh masyarakat luar yang banyak mengakses jaringan internet mengakibatkan munculnya beberapa masalah ketika jaringan tersebut digunakan yaitu koneksi jaringan lambat. Sejauh ini belum terdapat sistem keamanan yang dapat melakukan analisis, sehingga serangan yang terja di dapat bedampak fatal pada server.

Melihat permasalahan diatas pada SMKN 1 Palopo membutuhkan sebuah sistem keamanan jaringan pada jaringan sekolah untuk menghindari serangan dari pihak luar yang tidak bertanggung jawab. Hal tersebut dilakukan supaya semua pengguna internet bisa melakukan akses jaringan merasa aman didalam menggunakan internet. Sehingga dirancang keamanan jaringan komputer menggunakan model forensik untuk dapat mengetahui serangan terhadap jaringan sekolah. Dari penjelasan di atas, penulis sangat berminat melakukan untuk mempelajari dalam hal pemasangan keamanan jaringan pada SMKN 1 Palopo. Sehubungan dengan hal tersebutlah penulis untuk melakukan penelitian yang berjudul "Implementasi Keamanan Jaringan Komputer Dengan Menggunakan Model Forensik pada SMK Negeri 1 Palopo", sehinggga dapat untuk membantu sekolah dalam mengamankan jaringan komputer kepada siswa, guru dan staff yang ada di sekolah.

Metode

Jenis Penelitian yang digunakan dalam penelitian ini yaitu penelitian kuantitatif. Penelitian kuantitaif adalah salah satu jenis penelitian yang bertujuan untuk menjelaskan apa yang sebenarnya terjadi dalam situasi saat ini yang sedang diselidiki. Metode penelitian kuantitatif dipilih karena penelitian deskriptif kuantitatif adalah penelitian yang menggunakan observasi, wawancara, atau kuesioner tentang keadaan penelitian saat ini. Penelitian ini dilakukan di SMKN 1 Palopo Jl. KH. M. Kasim No. 10, Pattene, Kota Palopo. Adapun batasan dalam penelitian dilakukan agar berhasil memandu penelitian dalam waktu yang terbatas tergantung pada tujuan penelitian. Keterbatasan penelitian ini yaitu (1) Penelitian ini berfokus pada pengimplementasian proses model forensik pada jaringan komputer di SMK Negeri 1 Palopo, (2) Mengimplementasikan proses model forensik pada jaringan komputer di SMK Negeri 1 Palopo (3) Teknik pengujian menggunakan Model forensik, dan (4) Hasil yang di tampilkan berupa keamanan jaringan pada sekolah yaitu di SMK Negeri 1 Palopo.

Metode pengumpulan data yang digunakan untuk mengumpulkan data dalam wawancara survei kualitatif dan survei dokumenter berdasarkan konsep-konsep ini, diikuti oleh tiga teknik pengumpulan data diantaranya (1) Observasi, digunakan untuk mengamati secara langsung dan tidak langsung tentang sistem penerapan jaringan yang sedang berjalan di SMK Negeri 1 Palopo, guna merancang sistem jaringan yang akan diusulkan, (2) Wawancara, dipergunakan untuk mengadakan komunikasi dengan pihak-pihak terkait atau subjek penelitian, antara lain Kepala Sekolah selaku penaggung jawab dan Kepala Laboratorium komputer selaku administrator sistem dalam rangka memperoleh penjelasan atau informasi tentang hal-hal permasalahan dan kekurangan jaringan akan keamanan jaringan yang ada sekarang atau keterangan yang diperlukan dalam penelitian yang dilakukan di Sekolah Menengah Kejuruan Negeri 1 Palopo, (3) Studi pustaka, untuk mendapatkan materi yang dibutuhkan memperkuat pemahaman penulis dengan penelitian yang akan dilakukan, seperti buku, artikel, jurnal-jurnal penelitian yang telah dilakukan sebelumnya oleh peneliti.

Hasil

Hasil Wawancara dan Hasil Observasi

Penelitian dilakukan pada waktu dan tempat yang telah ditentukan. Sebelum melakukan investigasi, peneliti terlebih dahulu mewawancarai pengelola lab komputer yang bertanggung jawab atas pemeliharaan jaringan untuk menyelidiki beberapa masalah topologi dan jaringan internet SMK Negeri 1 Palopo. Kurangnya tekanan waktu untuk melakukan pemantauan saat melakukan fase pemantauan keamanan perangkat yang dapat mendeteksi serangan terhadap jaringan internet di sekolah, sehingga memudahkan orang lain diluar sekolah dalam mengakses internet secara ilegal.

Implementasi Hardware

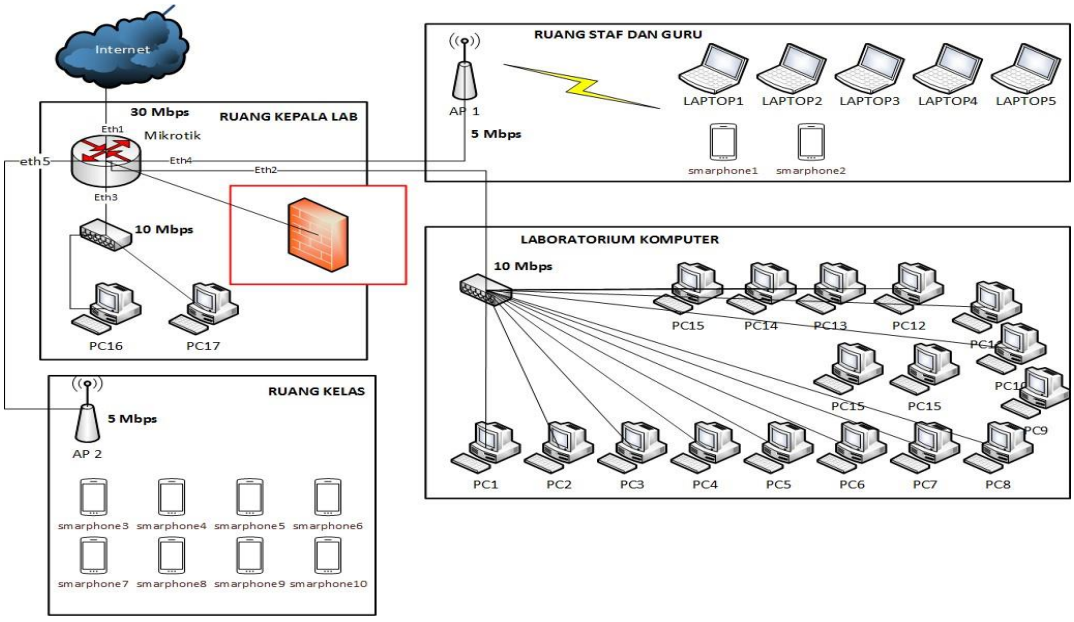
Ada beberapa Perangkat keras yang digunakan saat pengujian model forensik jaringan dengan SMK Negeri 1 Palopo : 1 buah Mikrotik, 1 buah switch HP V141014 24 port, 1 buah access point, 1 buah komputer PC sebagai server, 20 buah laptop PC dan lain-lain berbagai jenis perangkat. Hal pertama yang perlu Anda lakukan adalah memastikan bahwa semua perangkat Anda yang ada terhubung dengan kabel. Yaitu, hubungkan switch dan access point ke Mikrotik, dan sambungkan komputer lain ke switch dan access point. Saat menggunakan alamat IP di jaringan LAN menggunakan IP Network 192.168.10.0/26 Setiap perangkat diasumsikan memperoleh IP *Address* secara DHCP dari mikrotik. IP *Address* 192.168.10.1 digunakan di mikrotik, sedangkan untuk *client* yang terhubung ke *access point* menggunakan IP Address 192.168.50.2-192.168.50.254 yang dihubungkan melalui mikrotik yang digunakan.Apabila semua perangkat dipastikan terpasang dengan baik, maka langkah selanjutnya adalah melakukan pengujian jaringan komputer *LAN* dengan model forensik yang telah ditentukan.

Implementasi Perangkat Lunak

Pada fase ini penulis menyiapkan aplikasi yang digunakan untuk menyerang jaringan yang ada. Aplikasi yang digunakan adalah aplikasi LOIC berfungsi untuk menyerang komputer yang terkoneksi kedua jaringan komputer yang dibangun yaitu jaringan yang terkoneksi ke LAN melalui switch dan jaringan koneksi melalaui access point. Untuk memastikan jaringan yang ada pada SMK Negeri 1 Palopo memiliki kemananan yang baik.

Topologi Jaringan

Setelah dilakukan observasi dapat diketahui bahwa topologi jaringan yang lama ditambahkan sebuah perangkat mikrotik untuk melakukan *firewall* terhadap serangan dari dalam dan luar Jaringan SMK Negeri 1 Palopo sebagai berikut:



Gambar 1 Topologi Jaringan yang Diusulkan

Gambar 1 menunjukkan format cabang dari topologi jaringan LAN dan jaringan *wireless* yang digunakan di SMK Negeri 1 Palopo yaitu topologi jaringan *star* dimana seluruh ruangan terpusat ke ruang kepala laboratorium komputer. Berdasarkan hasil pengujian yang dilakukan dengan menjalankan beberapa serangan, hasil yang didapat berdasarkan pengujian yang dilakukan baik sebelum menggunakan sistem keamanan maupun setelah menggunakan sistem keamanan mikrotik pada jaringan. Dari sini, kita dapat menyimpulkan bahwa ini ditunjukkan pada tabel karena perbedaan analisis keamanan sebelum dan sesudah menggunakan proxy dibawah ini :

Tabel 4. Pengujian Menggunakan Model Forensik Terhadap Sistem Keamanan

No	Pengujian	Hasil Pengujian Hari/Tanggal	Status	Ket
1.	Deteksi Serangan DdoS	Senin 30/08/2021	Berhasil	Dapat menampilkan akses legal dan ilegal lewat mikrotik
2.	Pemeriksaan Serangan DdoS	Selasa 31/08/2021	Berhasil	Dapat memeriksa jumlah paket data yang terkirim
3.	Analisis Forensik Jaringan	Rabu 01/09.2021	Berhasil	Dapat mendeteksi akses tidak sah dan memberikan informasi lebih rinci ke menu obor untuk mengindikasikan serangan DDoS.
4.	Eksekusi	Kamis 02/09/2021	Berhasil	Dapat dilakukan pemblokiran IP Address agar pengguna dengan IP Address, tidak dapat melakukan serangan maupun membobol jaringan karena telah dilakukan pemblokiran

Pembahasan

Meriam ion orbit bumi rendah, juga dikenal sebagai LOIC, digunakan untuk menonaktifkan server situs web. Perangkat lunak DDOS yang paling kuat, kelas komunitas peretasan "anonim", telah terbukti menggunakan alat Loic ini untuk memulai tindakan. Setelah men*download software* nya, klik pada *software* loic.exe. Skenario survei ditunjukkan pada Lampiran 5. Saat Anda menghubungkan komputer pengguna model bintang ke sakelar dan titik akses, dan kemudian ke router secara bergantian, firewall dibuat sebagai sistem keamanan dan koneksi terakhir ke Internet. Jaringan tersebut dapat diakses dari dalam dan luar jaringan komputer SMK Negeri 1 Palopo. Untuk mensimulasikan serangan pada jaringan komputer, ruang guru dan lab komputer sekolah kemudian diserang menggunakan serangan DDoS menggunakan software LOIC. Serangan dilakukan dengan memasukkan alamat IP tujuan pada baris alamat IP. LOIC siap melakukan serangan terhadap target, layanan jaringan SMK Negeri 1 Palopo.

Dalam hal ini, pendeteksian serangan DDoS menggunakan software Winbox RouterOS untuk mengidentifikasi penyerang. Hijau menunjukkan akses yang sah dan merah menunjukkan akses tidak sah ke jaringan SMK Negeri 1 Palopo. Cara untuk melihat dapat dilakukan dengan cara pilih tab *Interface => Interface ether2* pada *toolbar winbox.* Maka akan muncul kotak *torch.*

Tampilan menunjukkan *interface* yang terhubung ke jaringan *access point* yang melakukan penyerangan 192.168.50.253 terhadap IP Address 192.168.10.62 untuk mencoba masuk ke komputer. Sedangkan untuk IP Address 192.168.50.251 pengguna jaringan biasa yang tidak melakukan serangan terhadap komputer lain yang ada pada jaringan. Pemeriksaan (*Examination*), pada fase ini, mencari informasi tersembunyi dan menemukan dokumen terkait. Cek dengan software Winbox RouterOS, seperti pengecekan urutan paket, jumlah paket data, dan lain-lain. Untuk memeriksa jumlah paket data yang terkirim dalam dilihat pada gambar diatas yang ditandai dengan warna merah, dapat kita lihat IP *Address* dan jumlah paket yang terkirim melalui *interface* ether2.

Setelah mendeteksi akses yang tidak sah, perangkat lunak Winbox RouterOS memberikan informasi lebih lanjut di menu Tourch. Ini menunjukkan serangan DDoS, yaitu alamat IP (192.168.50.253) tempat serangan terjadi, yaitu pada tanggal 8 Oktober 2021 Saat penyerangan pada port 80 terjadi, alasannya adalah port 80 terbuka. Selain pengumpulan bukti, dibuat sistem peramalan. Artinya, memblokir alamat IP penyerang untuk mencegah serangan yang sama terjadi di masa mendatang. Gambar 32 menunjukkan bahwa serangan berikutnya tidak dapat diluncurkan karena alamat IP 192.168.50.253 diblokir. Lampiran 6 No. 5 menunjukkan bahwa proses yang menghentikan permintaan serangan setelah memblokir dan paket data yang dikirim oleh penyerang dihentikan. Pemblokiran IP Address agar pengguna dengan IP Address 192.168.50.253 tidak dapat melakukan serangan maupun membobol jaringan karena telah dilakukan pemblokiran, sedangkan untuk IP Address 192.168.10.1 agar mikrotik tidak dapat diakses dari luar maupun dari dalam dan 192.168.0.1 untuk IP Address modem juga dilakukan pemblokiran.

Hasil Pengujian Jaringan

Pengujian yang dilakukan dalam uji beberapa percobaan menampilkan hasil yang cukup memuaskan. Hasil pengujian menunjukkan *client* tidak bisa connect ke IP *Address* yang sudah di blokir. Sehingga dapat dikatakan bahwa dengan penggunaan mikrotik dapat mengamankan jaringan dari serangan dalam dan luar baik melalui jaringan LAN dan *wireless* berhasil dan ini berfungsi dengan baik dan Anda dapat melihat semua hasil pengujian sistem pada tabel berikut:

Tabel 5. Hasil pengujian implementasi keamanan jaringan

No	Pengujian	Hasil Pengujian		Keterangan
		Berhasil	Gagal	
1	Akses Mikrotik Lewat winbox		Ö	Tidak dapat akses mikrotik lewat Winbox
2	Akses modem lewat browser		Ö	Tidak dapat akses modem lewat Winbox
3	Serangan DDOS lewat Loic		Ö	Tidak dapat melakukan serangan DDOS lewat Loic

Melakukan tes metode forensik ini adalah uji beberapa percobaan yang dilakukan ke router mikrotik, modem internet dan serangan menggunakan *software* LOIC untuk menampilkan hasil apakah pemblokiran yang dilakukan berhasil serta dapat mengamankan jaringan dari serangan dari dalam dan luar jaringan di SMK Negeri 1 Palopo yang melalaui koneksi *LAN* dan *wireless*. Untuk selanjutnya dilakukan pemblokiran mac address agar jaringan kita aman dari serangan pembobol jaringan melalui jaringan LAN maupun jaringan *wireless.* Pemblokiran IP Address yang sering melakukan koneksi ke jaringan secara ilegal. Untuk melihat apakah pemblokiran IP *Address* dan mac *address* berhasil atau peneliti akan coba melakukan login ke winbox mikrotik dan login ke modem pada *browser.*

Kesimpulan

Berdasarkan hasil pengujian dan implementasi motede forensik Sistem keamanan jaringan komputer dapat dirancang menggunakan bukti forensik jaringan komputer. Setelah pengenalan sistem keamanan jaringan komputer, penyerang tidak akan dapat melakukan serangan menggunakan metode yang sama di masa depan. Dengan mikrotik, Anda berhasil melindungi jaringan Anda dari serangan **i**nternal dan eksternal melalui jaringan LAN dan nirkabel, dan berfungsi dengan baik.

References

Abdul Wahab, Solichin. (2002). Analisis Kebijaksanaan: dari Formulasi ke Implementasi Kebijaksanaan Negara, Sinar Grafika, Jakarta.

Al-Bahra Bin Ladjamudin. (2013). Analisis dan Desain Sistem Informasi. Graha Ilmu. Yogyakarta.

Farhat, F. (2008). Tahapan Komputer Forensik. Universitas Gunadarma.

Firrar Utdirartatmo. (2005). Teknik Kompilasi, Graha Ilmu, Yogyakarta.

Harsono, H. (2002). Implementasi Kebijakan dan Politik. Jakarta.

I. Riadi. (2011). Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik Pendahuluan Landasan Teori. JUSI, Univ. Ahmad Dahlan Yogyakarta, 1(1), 71–80

Iswandy & Eka. (2015). Sistem Penunjang Keputusan Untuk Menentukan Penerimaan Dana Santunan Sosial Anak Nagari Dan Penyalurannya Bagi Mahasiswa Dan Pelajar Kurang Mampu Di Kenagarian Barung – Barung Balantai Timur. Jurnal Dosen Sekolah Tinggi Manajemen Informatika Komputer STMIK Jayanusa Padang. 3(3), 73.

Gunawan, H., Simorangkir, H., Ghiffari, M., Informatika, T., Komputer, F. I., & Unggul, U. E. (2018). Pengelolaan Jaringan Dengan Router Mikrotik Untuk Meningkatkan Efektifitas Penggunaan Bandwith Internet (Studi Kasus Smk Ki Hajar Dewantoro Kota Tangerang), 3(1), 54–70.

Kristanto, A. (2003). Jaringan Komputer. Yogyakarta: Graha Ilmu. Kurniawan, Wiharsono. 2007. Jaringan Komputer. Semarang: Andi

Kusuma Dewi, E., & Kasih, P. (2017). Meningkatkan Keamanan Jaringan dengan Menggunakan Model Proses Forensik. Seminar Nasional Teknologi Informasi Komunikasi dan Aplikasinya (SNATIKA), pp. 167-172.

Kusuma Dewi, E. (2016). Rancangan Keamanan Jaringan Dengan Menggunakan Model Proses Forensik. Jurnal Maklumatika, 2(2)

Kusuma Dewi, E., & Kasih, P. (2017). Analisis Log Snort Menggunakan Model Proses Forensic. Jurnal Ilmiah Penelitian dan Pembelajaran Informatika (JIPI) STKIP Tulungagung,, 2(2), 72-79.

Kuswayanto, L. (2008). Mahir Dan Terampil Berkomputer. Jakarta: Grafindo Media Pratama.

Limbuna Yosti. (2015) Implementasi Billing Hotspot Menggunakan Fitur User Manager Di Mikrotik Pada Warnet Dahlia Raya. (Doctoral dissertation, Universitas Cokroaminoto Palopo)

Lukas & Jonathan. (2006). Jaringan Komputer. Jakarta: Graha Ilmu.

Ma'sum, M. S., Irwansyah, M. A., & Priyanto, H. (2017). Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter. JUSTIN (Jurnal Sistem dan Teknologi Informasi), 5(1), 56-60.

Moch. Linto Herlambang, Azis Catur L. (2008). Panduan Lengkap Menguasai Router Masa Depan Menggunakan MikroTik RouterOSTM, Yogyakarta: Penerbit ANDI Yogyakarta.

Muhajir Imam. (2014). Tugas Makalah Jaringan Komputer. Universitas ulum Jombang.

Nugroho, B. A. (2012). Analisis Keamanan Jaringan Pada Fasilitas Internet (WiFi) Terhadap Serangan Packet Sniffing (Doctoral dissertation, Universitas Muhammadiyah Surakarta).

R. Utami and J. Istiyanto, Eko. (2012). Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada. vol. 6, no. 2, pp. 101–112, 2012.

Samsumar & Hadi. (2017). Analisis dan Evaluasi Tingkat Jaringan Komputer Nirkabel (Wireless LAN) Studi Kasus Kampus STMIK Mataram. Jurnal Ilmiah Teknologi Terapan.

Setiawan, G. (2004). Implementasi Dalam Birokrasi Pembangunan. Jakarta.

Singh O. (2009). Network Forensics. Indian Computer Response Team (CERT-In) Department of Information Technology, New Delhi, India.

Sofana, Iwan (2012). Cisco CCNP dan Jaringan Komputer. Bandung: Informatika. Sulianta, F. 2013. Komputer Forensik. Elex Media Komputindo.

Sulianta, F. (2016). forensik komputer - melacak kejahatan digital. Penerbit Andi: Yogyakarta

Usman, N. (2002). Konteks Implementasi Berbasis Kurikulum. Jakarta

Yani, A. (2007). Panduan Membangun Jaringan Komputer. Jakarta: Kawan Pustaka.