

**MONITORING KEAMANAN JARINGAN DENGAN SNORT IDS  
MENGUNAKAN METODE FORENSIC JARINGAN  
(STUDI KASUS: CV.TRIEM GUNUNG MAS SEJAHTERA)**

**SKRIPSI**

**Program Studi Teknik Informatika**



**NAMA : BUDI MULYA AJI PRASETYO  
NIM : 011501503125067**

**FAKULTAS TEKNIK**

**UNIVERSITAS SATYA NEGARA INDONESIA**

**2019**

**MONITORING KEAMANAN JARINGAN DENGAN SNORT IDS  
MENGUNAKAN METODE FORENSIC JARINGAN  
(Studi Kasus: CV.Triem Gunung Mas Sejahtera)**

**SKRIPSI**

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar  
Sarjana Komputer  
Program Studi Teknik Informatika**



**UNIVERSITAS SATYA NEGARA INDONESIA**

**2019**

## ABSTRAK

### Monitoring Keamanan Jaringan Dengan Snort IDS Menggunakan Metode Forensic Jaringan (Studi Kasus: CV.Triem Gunung Mas Sejahtera)

Budi Mulya Aji Prasetyo

011501503125067

Universitas Satya Negara Indonesia

Email: [ajibudi2996@gmail.com](mailto:ajibudi2996@gmail.com)

Penelitian ini dilakukan pada perusahaan CV Triem Gunung Mas Sejahtera dan menemukan permasalahan yang terjadi pada perusahaan tersebut yaitu tidak adanya keamanan jaringan komputer server. Salah satunya adalah serangan terhadap komputer target ini bisa mengakibatkan kerusakan pada komputer seperti server mengalami hang atau melakukan *reboot*, ini bisa menghambat pekerjaan dan dapat merugikan perusahaan.

Keamanan jaringan merupakan faktor penting untuk menjamin data dari pencurian atau pengrusakan data. Dengan meningkatnya pengetahuan tentang *hacking* dan *cracking* serta di dukung banyaknya *tools* yang bisa digunakan secara mudah untuk melakukan serangan atau penyusupan. Ketika serangan terjadi, maka perlu dilakukan investigasi. Salah satu metode forensic jaringan untuk memonitoring serangan terhadap jaringan menggunakan *Snort IDS*.

Untuk mengantisipasi serangan tersebut supaya tidak terjadi pada perusahaan CV Triem Gunung Mas Sejahtera, untuk itu di butuhkan metode *forensic* jaringan salah satunya adalah *snort IDS*. Untuk keamanannya menggunakan *Netcut* dan Mikrotik sebagai firewallnya. Perangkat lunak ini memudahkan admin jaringan dalam memanajemen sebuah keamanan jaringan komputer. Snort telah berhasil memonitoring dan melakukan investigasi serangan. Dan sebagai tambahan keamanan *Netcut* dan Mikrotik telah berhasil memblokir ip penyerang, maka dapat disimpulkan bahwa sistem keamanan jaringan komputer server CV. Triem Gunung Mas Sejahtera sudah cukup aman.

Kata kunci: *Snort IDS*, *Forensic* Jaringan, *Netcut*, Mikrotik

## ABSTRACT

*Network Security Monitoring With IDS Snort Using Forensic Network Method  
(Case Study: CV. Tri Gunung Mas Sejahtera)*

**Budi Mulya Aji Prasetyo**  
**011501503125067**  
**Satya Negara Indonesia University**

**Email: [ajibudi2996@gmail.com](mailto:ajibudi2996@gmail.com)**

*This research was conducted at the company CV Triem Gunung Mas Sejahtera and found problems that occur in the company that is the absence of server computer network security. One of them is that the attack on the target computer can cause damage to the computer such as the server hangs or reboots, this can hamper work and can harm the company.*

*Network security is an important factor to guarantee data from theft or destruction of data. With increasing knowledge about hacking and cracking and supported by the many tools that can be used easily to carry out attacks or infiltrations. When an attack occurs, an investigation is needed. One of the network forensic methods is to monitor attacks on the network using Snort IDS.*

*To anticipate the attack so that it does not happen to the company CV Triem Gunung Mas Sejahtera, for that network forensic method is needed one of them is snort IDS. For security use Netcut and Mikrotik as a firewall. This software makes it easy for network admins to manage a computer network security. Snort has successfully monitored and investigated attacks. And in addition to security Netcut and Mikrotik have successfully blocked the attacker's ip, it can be concluded that the CV server computer network security system. Gunung Mas Sejahtera Triem is safe enough.*

*Keywords: IDS Snort, Forensic Network, Netcut, Microtic*