

**PROGRAM STUDI TEKNIK KOMPUTER**

**ANALISA MONITORING UNTUK PENCEGAHAN AKSES**

**ILEGAL DI DALAM JARINGAN DEPARTEMEN TI**

**PT.PUPUK SRIWIDJAJA PALEMBANG**

**KARYA AKHIR**



**M.ALZI IKRAR AGAMURI**

**201220020**

**PROGRAM DIPLOMA III**

**FAKULTAS VOKASI**

**UNIVERSITAS BINA DARMA**

**PALEMBANG**

**2023**



**ANALISA MONITORING UNTUK PENCEGAHAN AKSES  
ILEGAL DI DALAM JARINGAN DEPARTEMEN TI  
PT.PUPUK SRIWIDJAJA PALEMBANG**

**M.ALZI IKRAR AGAMURI**

**201220020**

**Karya akhir ini diajukan sebagai salah satu syarat memperoleh gelar**

**Ahli Madya (A.Md.)**

**PROGRAM STUDI TEKNIK KOMPUTER**

**FAKULTAS VOKASI**

**UNIVERSITAS BINA DARMA**

**PALEMBANG**

**2023**

**HALAMAN PENGESAHAN**

**ANALISA MONITORING UNTUK PENCEGAHAN AKSES  
ILEGAL DI DALAM JARINGAN DEPARTEMEN TI PT PUPUK  
SRWIDJAJA PALEMBANG  
M.ALZI IKRAR AGAMURI**

**201220020**

Telah diterima sebagai salah satu syarat untuk memperoleh gelar Ahli Madya  
pada Program Studi Teknik Komputer

Palembang 9 September 2023

Fakultas vokasi

Universitas Bina Darma Palembang

Pembimbing

(Tamsir Ariyadi M.kom)

Dekan

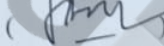

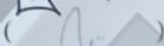
Fakultas Vokasi

(Dr.A.Yani Rainus.,S.Kom., M.M)

## HALAMAN PERSETUJUAN KOISI PENGUJI

Karya akhir Berjudul “Analisa Monitoring Untuk Pencegahan Akses Ilegal Di Dalam Jaringan Departemen Ti Pt. Pupuk Sriwidjaja Palembang” oleh M.Alzi Ikrar Agamuri di depan komisi penguji pada hari Sabtu tanggal 9 September 2023

### KOMISI PENGUJI

- |                          |                    |   |
|--------------------------|--------------------|---|
| 1. Tamsir ariyadi M.kom. | Ketua Penguji      | (  ) |
| 2. Irwansyah M.M.,M.Kom. | Anggota Penguji I  | (  ) |
| 3. Misinem S.Kom., M.Si. | Anggota Penguji II | (  ) |

Palembang, 9 September 2023

Program Studi Teknik Kompter

Universitas Bina Darma

Ketua,

Universitas Bina Darma  
Fakultas Voks

(Timur Dali Purwanto, M.Kom)

## SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama : M. Alzi Ikrar Agamuri  
NIM : 201220020

Dengan ini menyatakan bahwa:

1. Karya Akhir ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik Ahli Madya di Universitas Bina Darma;
2. Karya tulis ini murni gagasan, rumusan dan penelitian saya sendiri dengan arahan pembimbing;
3. Di dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dikutip dengan mencantumkan nama pengarang dan memasukkannya ke dalam daftar pustaka;
4. Saya bersedia Karya Akhir yang saya hasilkan dicek keasliannya menggunakan plagiarism checker dan diunggah ke internet, sehingga dapat diakses publik secara daring.
5. Surat pernyataan ini saya tulis dengan sungguh-sungguh dan apabila terbukti melakukan penyimpangan atau ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi dengan peraturan dan perundang-undangan yang berlaku.

Demikian surat pernyataan ini saya buat agar dapat di pergunakan sebagaimana mestinya.

Palembang, 9 September 2023  
Yang membuat pernyataan,



M. Alzi Ikrar Agamuri  
NIM : 201220020

## MOTTO DAN PERSEMBAHAN

### MOTTO :

- Atas Kehendakmu dan Ridhomu Allah SWT aku melangkah bersamamu untuk menentukan masa depan terbaikku.
- *Success doesn't have to be a rich person, success is when you don't think too much about the world and focus on doing good deeds for the afterlife.*

### PERSEMBAHAN:

- Allah SWT yang memberikan jalan dan hidayahnya.
- Kedua Orang Tua tercinta Ayahku (Defransa) dan Ibuku (Afrida) yang tak pernah berhenti memberikan dukungan moril dan materil serta selalu berdo'a demi keberhasilanku.
- Kepada Saudariku (Lolita Salsa Bila Monica) terima kasih atas suport dan dukungannya serta do'anya.
- Kepada adikku yang tercinta ( Faiz ) yang selalu mendoakandan tak pernah hent memberikan dukungan.
- Kepada jinan selaku teman baik saya yang paling cantik tiada henti memberikan dukungan dengan tulus untuk menyelesaikan Karya Akhir ini.
- Sahabat virus A3 (Aidil Nur Riyansyah, dan M.Agung) .

## ABSTRACT

Technology plays an important role in human survival in daily activities cannot be separated from technology. Information technology makes it easy for humans to share information or find information. Cyberattacks such as malware attacks or hacking attempts pose a serious threat to IT networks. The purpose of network security is to anticipate the risk of network threats that can disrupt daily computer network operations. In this study the author uses the Action Research method. Davison, et al (2004) This Reaction Research method aims at testing and development, finding and designing, these steps are applied in the workplace (Object), By using this method the work will be younger, faster and the results are better and more qualified.

**Keywords :** Wireshark, Monitoring, Technology, PT. Pusri

## ABSTRAK

Teknologi memegang peranan penting kelangsungan hidup manusia dalam aktivitas sehari-hari tidak lepas dari teknologi. Teknologi informasi memudahkan manusia berbagi informasi atau mencari informasi. Serangan siber seperti serangan *malware* atau upaya peretasan merupakan ancaman serius bagi jaringan TI. Tujuan dari keamanan jaringan adalah untuk mengantisipasi resiko ancaman jaringan yang dapat mengganggu operasional jaringan komputer sehari-hari. Dalam penelitian kali ini penulis menggunakan metode *Action Research*. Davison, et al (2004) Metode *Reaction Research* ini di bertujuan untuk pengujian dan pengembangan, menemukan dan merancang, langkah-langkah ini diterapkan di tempat kerja (Objek), Dengan menggunakan metode ini pekerjaan akan menjadi lebih muda, lebih cepat dan hasilnya lebih baik dan lebih berkualitas.

**Kata Kunci :** Wireshark, Monitoring, Teknologi, PT.Pusri



# DAFTAR RIWAYAT HIDUP

## CURICULUM VITAE

**M. ALZI IKRAR AGAMURI, A.Md.**

**Fresh Graduate, Computer Engineering of Universitas Bina Darma**

PALEMBANG, SOUTH SUMATERA 30656- 0822-8051-1854 -Email : [alziikrar@gmail.com](mailto:alziikrar@gmail.com)

### PERSONAL INFORMATION

Date Of Birtd : Palembang, january, 26<sup>th</sup>, 2002  
Address : Lr.Gubah Rt.33 Rw.10 kecamatan Bukit  
Kecil Kelurahan 26 Ilir  
Nationality : Indonesia  
Material Status : Single

3 x 4

### EDUCATION BACKGROUND

**2020 – 2023**      **Universitas Bina Darma**  
Vocational Faculty  
Computer Enginnering  
Associate's degree

### AWARD

**2022**      **Participant of Businnes Plan Competition Ganjil 2022**  
**Bina Darma University**

## KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Puji dan syukur saya panjatkan kepada Allah subhanahu wa ta'ala atas ridhonya sehingga saya dapat menyelesaikan Karya Akhir ini tepat pada waktunya. Ini merupakan salah satu syarat untuk memperoleh gelar Ahli Madya pada Program Studi Teknik Komputer Universitas Bina Darma Palembang. Dengan Judul Karya Akhir yaitu ” Analisa Monitoring Untuk Pencegahan Akses Ilegal Di Dalam Jaringan Departemen Ti Pt.Pupuk Sriwidjaja Palembang

Dalam proses pengerjaan Karya Akhir ini, tidak dapat disangkal bahwa butuh usaha yang keras dan juga niat yang sungguh-sungguh agar lapoaran penelitian ini diselesaikan. Namun, penulis juga menyadari bahwa Karya Akhir ini tidak akan selesai tanpa bantuan dari berbagai pihak yang senantiasa bersedia meluangkan waktunya untuk mendukung dan membimbing penulis. Oleh karena itu pada kesempatan kali ini penulis ingin mengucapkan terimakasih kepada semua pihak yang telah berkenaan membantu baik secara moril maupun materil dalam penulisan penelitian ini. Dengan segala hormat dan rasa syukur yang dalam, menyampaikan rasa terimakasih yang sebesar-besarnya kepada :

1. Kepada Orangtuaku tercinta dan kusayangi Papa dan Mama yang telah merawatku dari kecil sampai memperoleh gelar Ahli Madya.
2. Prof. Dr. Sunda Ariana, M.Pd., M.M. Selaku Rektor Universitas Bina Darma Palembang.
3. Dr. A. Yani Ranius, S.Kom., M.M. Selaku Dekan Fakultas Vokasi.
4. Timur Dali Purwanto M.Kom. Selaku Ketua Program Studi Teknik Komputer.
5. Rahmat Novrianda Dasmen, S.T., M.Kom. Selaku Dosen Pembimbing yang telah memberikan arahan dan bimbingan dalam proses untuk menyelesaikan Karya akhir ini, sekaligus Selaku Pembimbing lapangan dalam kegiatan magang di Direktorat Inovasi dan Inkubator Bisnis (DIIB). Terima kasih atas saran-saran yang telah diberikan.

6. Dosen Penguji, serta seluruh dosen di Universitas Bina Darma khususnya Dosen Teknik Komputer.
7. Teman-teman seperjuangan yang banyak memberikan masukan serta bantuan dalam menyelesaikan Karya Akhir ini.

Semoga segala bantuan yang telah diberikan kepada penulis mendapatkan balasan yang lebih besar dari Allah subhanahu wa ta'ala. Demikian Laporan ini penulis susun dengan harapan dapat bermanfaat bagi penulis khususnya dan bagi pembaca umumnya.

Palembang, 9 September 2023



M. Alzi Ikrar Agamuri

## DAFTAR ISI

<b>HALAMAN PENGESAHAN</b> .....	<b>ii</b>
<b>HALAMAN PERSETUJUAN KOISI PENGUJI</b> .....	<b>iii</b>
<b>SURAT PERNYATAAN</b> .....	<b>iv</b>
<b>MOTTO DAN PERSEMBAHAN</b> .....	<b>v</b>
<b>ABSTRACT</b> .....	<b>vi</b>
<b>ABSTRAK</b> .....	<b>vii</b>
<b>DAFTAR RIWAYAT HIDUP</b> .....	<b>viii</b>
<b>KATA PENGANTAR</b> .....	<b>ix</b>
<b>BAB I</b> .....	<b>1</b>
<b>PENDAHULUAN</b> .....	<b>1</b>
<b>1.1 Latar Belakang</b> .....	<b>1</b>
<b>1.2 Rumusan Masalah</b> .....	<b>4</b>
<b>1.3 Batasan masalah</b> .....	<b>4</b>
<b>1.4 Tujuan Dan Manfaat Penelitian</b> .....	<b>5</b>
1.4.1 Tujuan penelitian.....	5
1.4.2 Manfaat penelitian.....	5
<b>1.5 Penelitian Terdahulu</b> .....	<b>7</b>
<b>BAB II</b> .....	<b>10</b>
<b>METODOLOGI PENELITIAN</b> .....	<b>10</b>
<b>2.1 Gambaran Objek Penelitian</b> .....	<b>10</b>
2.1.1 Profil Instansi .....	10
2.1.2 Visi dan Misi Instansi .....	11
2.1.3 Struktur Grup Instansi .....	12
2.1.4 Makna Lambang .....	13
2.1.5 Filosofi Nama Instansi .....	14
2.1.6 Detail Elemen Visual Logo instansi.....	15

2.1.7	Identitas Instansi.....	17
2.1.8	Struktur Organisasi PT Pusri Palembang.....	19
2.1.9	Sistem Manajemen dan Struktur Organisasi Departemen Mitra Bisnis dan Layanan TIPSP .....	21
<b>2.2</b>	<b>Monitoring .....</b>	<b>22</b>
<b>2.3</b>	<b>Analisis .....</b>	<b>22</b>
<b>2.4</b>	<b>Pengertian mencegah .....</b>	<b>23</b>
<b>2.5</b>	<b>Wireless .....</b>	<b>23</b>
<b>2.6</b>	<b>Web Traffic .....</b>	<b>23</b>
<b>2.7</b>	<b>Cyber Crime.....</b>	<b>24</b>
<b>2.8</b>	<b>Jaringan Komputer .....</b>	<b>24</b>
<b>2.9</b>	<b>Keamanan Jaringan .....</b>	<b>24</b>
<b>2.10</b>	<b>Wireshark.....</b>	<b>24</b>
<b>2.11</b>	<b>Metode Penelitian .....</b>	<b>25</b>
2.11.1	Diagnose (Diagnosis).....	25
2.11.2	Alat Alat yang Digunakan Topologi Pada PT. Pupuk Srwiridjaja .....	26
2.11.3	Topologi Jaringan PT.Pupuk Sriwidjaja Palembang .....	28
2.11.4	Topologi jaringan departemen TI.....	30
2.11.5	Rencana Tindakan (Action Planing).....	30
2.11.5	Evaluasi (Evaluating) .....	31
<b>2.12</b>	<b>Rancangan Penelitian.....</b>	<b>31</b>
<b>BAB III.....</b>	<b>.....</b>	<b>33</b>
<b>HASIL DAN PEMBAHASAN.....</b>	<b>.....</b>	<b>33</b>
<b>3.1</b>	<b>Hasil .....</b>	<b>33</b>
3.1.1	Hasil Monitoring <i>Wireshark</i> .....	33
3.1.2	Filtering Protokol HTTP.....	34
<b>3.2</b>	<b>Analisis .....</b>	<b>38</b>
<b>3.2</b>	<b>Pembahasan .....</b>	<b>41</b>
<b>BAB IV .....</b>	<b>.....</b>	<b>42</b>
<b>KESIMPULAN DAN SARAN .....</b>	<b>.....</b>	<b>42</b>

4.1	Kesimpulan .....	42
4.2	Saran.....	42
	Daftar Pustaka.....	44



## DAFTAR TABEL

<b>Tabel 2. 1</b> Makna Logo Pusri.....	17
<b>Tabel 3. 1</b> Website yang di akses pengguna pada jaringan PT.Pusri.....	40
<b>Tabel 3. 2</b> data ip akses protocol http.....	40



## DAFTAR GAMBAR

<b>Gambar 2.1</b> Struktur Grup Pusri 1 .....	12
<b>Gambar 2.2</b> Logo Pusri 1.....	14
<b>Gambar 2.3</b> Struktur Organisasi PT. Pusri 1 .....	20
<b>Gambar 2.4</b> Struktur Organisasi PT. Pusri 1 .....	20
<b>Gambar 2.5</b> Struktur Organisasi PT.Pusri. 1 .....	21
<b>Gambar 2.6</b> Struktur Departemnet Mitra B 1 .....	22
<b>Gambar 2.7</b> Metode Acion Research 1 .....	25
<b>Gambar 3. 1</b> filtering protokol http pada jaringan pusri.id new.....	34
<b>Gambar 3. 2</b> filtering protokol http pada jaringan KM-LABKOM .....	35
<b>Gambar 3. 3</b> Tcp Stream .....	36
<b>Gambar 3. 4</b> filtering protokol http pada jaringan diklat .....	36
<b>Gambar 3. 5</b> tcp Stream .....	37
<b>Gambar 3. 6</b> Pertukaran Data .....	38
<b>Gambar 3. 7</b> TCP Stream.....	39
<b>Gambar 3. 8</b> Proses Komunikasi Data 1 .....	41



## DAFTAR LAMPIRAN

- Lampiran 1.** Logbook Magang
- Lampiran 2.** Nilai Magang
- Lampiran 3.** Permohonan Pengajuan Judul Karya Akhir
- Lampiran 4.** SK Pembimbing Karya Akhir
- Lampiran 5.** Lembar Konsultasi Karya Akhir
- Lampiran 6.** Lembar Perbaikan Karya Akhir

Universitas Bina  
Dharma



# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Di era digitalisasi saat ini, teknologi memegang peranan penting kelangsungan hidup manusia dalam aktivitas sehari-hari tidak lepas dari teknologi. masalah ini berubah dari cara berpikir menjadi acuan bagi kemajuan peradaban manusia dan menangani dan memecahkan setiap masalah pola pikir yang kompleks agar tidak tersesat dengan perkembangan dan dukungan teknologi informasi didukung oleh berbagai penemuan dan inovasi banyak perubahan dalam hidup seseorang. Itu juga menyebabkan pengembangan bersama pembangunan dan teknologi Perangkat keras, secara langsung atau tidak langsung Informasi telah menjadi bagian penting dalam berbagai aspek kehidupan untuk dukungan sederhana tenaga kerja manusia. Departemen TI seringkali bertanggung jawab untuk mengelola dan menjaga keamanan data sensitif seperti informasi karyawan, informasi pelanggan, atau data bisnis penting lainnya. Monitoring dan pencegahan akses ilegal membantu mencegah upaya pencurian atau pengungkapan data yang tidak sah di PT Pupuk Sriwidjaja (PUSRI).

Teknologi informasi memudahkan manusia berbagi informasi atau mencari informasi. kamu bisa melihatnya Tentang perkembangan teknologi internet dan jaringan. Baru-baru ini *internet* adalah untuk pertukaran informasi dan untuk mencari informasi. Jaringan komputer adalah suatu sistem yang terdiri dari dari beberapa komputer yang dirancang untuk pertukaran data, informasi dan sumber daya. Jaringan

komputer adalah suatu sistem yang terdiri dari beberapa komputer yang dirancang untuk pertukaran data, informasi dan sumber daya. Tujuan dari jaringan komputer adalah Setiap bagian dari jaringan komputer dapat meminta dan menyediakan layanan informasi dan data. Pihak yang meminta atau menerima layanan kepada siapa pelanggan merujuk dan siapa yang mengirim atau menyampaikan layanan disebut *server*.

Serangan siber seperti serangan *malware* atau upaya peretasan merupakan ancaman serius bagi jaringan TI. Dengan memantau lalu lintas jaringan dan menerapkan tindakan pencegahan yang tepat, departemen TI dapat mengidentifikasi serangan yang sedang berlangsung dan mengambil tindakan untuk menghentikannya sebelum menjadi sangat merusak bagi perusahaan. Pada pasal 30 ayat 1 UU ITE No 19 Tahun 2016, Perbuatan ini dapat dikategorikan yang dinyatakan dalam Pasal 30 ayat

(1) UU ITE yaitu setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun.

Tujuan dari keamanan jaringan adalah untuk mengantisipasi resiko ancaman jaringan yang dapat mengganggu operasional jaringan komputer sehari-hari. Nirkabel diperlukan di kantor karena nirkabel dapat membantu menyelesaikan pekerjaan.

Perkembangan teknologi *Wireless Fidelity (WI-FI)* mengalami kemajuan yang sangat pesat untuk memenuhi kebutuhan sistem. Teknologi *WI-FI* banyak digunakan pada *hotspot* komersial, keamanan jaringan Internet *Service Provider (ISP)* di sekolah dan perkantoran sangat penting, namun hanya sebagian operator jaringan saja yang memperhatikan keamanan lalu lintas data pada jaringan *WI-FI*. Salah satu ancaman

keamanan jaringan paling umum yang ditimbulkan oleh penjahat dunia maya adalah serangan paket. *Sniffing* paket adalah bentuk serangan yang menangkap data dari paket yang melintasi jaringan. Informasi ini mungkin termasuk nama pengguna, kata sandi, dan informasi penting lainnya yang dikirimkan melalui jaringan dalam bentuk teks. Tidak hanya satu paket yang harus ditangkap, bisa ratusan bahkan ribuan. Hal ini dapat merugikan pengguna jaringan komputer. Sero, R. L. (2022).

Dalam lingkungan TI yang kompleks, penggunaan ilegal atau aktivitas jaringan yang mencurigakan dapat mengganggu ketersediaan sistem. Dengan menggunakan solusi pemantauan yang tepat, departemen TI dapat mengidentifikasi masalah dan kesalahan jaringan dengan lebih cepat dan mengambil tindakan segera untuk menjaga ketersediaan sistem, Serangan yang berhasil dapat mengakibatkan gangguan pada proses bisnis. Mengontrol dan mencegah penggunaan ilegal dapat meminimalkan risiko kerusakan finansial dan reputasi yang mungkin diakibatkan oleh serangan atau pelanggaran keamanan.

Dalam penelitian ini penulis melakukan penelitian dengan menggunakan metode Action Research yang bertujuan untuk mengembangkan keterampilan-keterampilan baru atau cara-cara pendekatan baru dan untuk memecahkan masalah dengan cara penerapan langsung pada objek penelitian. Febriani, Y., & Sahfitri, V. (2022, August).

Sehubungan dengan hal tersebut di atas PT. Pupuk Sriwidjaja Palembang di perlukannya melakukan *monitoring* dan pencegahan dari akses illegal pada jaringan menggunakan *wireshark*. *Administrator* jaringan dapat mengabil tindakan

penaggulangan ketika akses ilegal terdeteksi melalui jaringan komputer akses ilegal yang di maksud adalah seperti pengguna atau user membuka situs atau webstie yang berbahaya dan tingkat keamanannya sangat lemah, Oleh karena itu *administrator* memerlukan alat yang tepat untuk memantau jaringan yaitu *wireshark*, *Software Wireshark* karena alat ini mampu menangkap paket data atau informasi dan sekaligus memantau lalu lintas antara Wlan (*Wireless Local area Network*). Febriani, Y., & Sahfitri, V. (2022, August).

Berdasarkan yang di jelaskan di latar belakang penulis tertarik memonitor dan mencegah akses ilegal di dalam jaringan, department TI dapat meningkatkan keamanan jaringan, melindungi data sensitif, mengurangi resiko serangan siber dan menjaga kelangsungan bisnis organisasi yang berjudul “*Monitoring Dan pencegahan Akses Ilegal Di Dalam Jaringan Pada Departemen TI Di PT Pupuk Sriwidjaja*”

## **1.2 Rumusan Masalah**

Berdasarkan dari latar belakang di atas, dirumuskan masalah pokok penelitian adalah “Bagaimana *Monitoring* jaringan dari akses ilegal pada PT Pupuk sriwidjaja dari akses ilegal Menggunakan *Wireshark*”?.

## **1.3 Batasan masalah**

Dengan rumusan masalah tersebut maka akan di buat dengan batasan masalah sebagai berikut:

1. Monitoring dengan menggunakan wireshark dapat dibatasi hanya pada perangkat yang dapat di akses dari titik wifi tertentu
2. Pada jaringan wida di gedung anex PT.Pupuk Sriwidjaja, monitoring hanya pada jaringan yang diidentifikasi dengan SSID tertentu yang ada di gedung tersebut
3. Waktu yang di gunakan dalam monitoring dari tanggal 6 juni – 21 juni 2023 juga bisa menjadi pertimbangan untuk melakukan monitoring lalu lintas jaringan pada gedung tersebut.

#### **1.4 Tujuan Dan Manfaat Penelitian**

##### **1.4.1 Tujuan penelitian**

Adapun tujuan penelitian ini adalah untuk memonitoring jaringan di PT Pupuk Sriwidjaja dari akses illegal menggunakan *wireshark*

##### **1.4.2 Manfaat penelitian**

Wireshark memungkinkan kita untuk menganalisis lalu lintas jaringan secara mendalam. Dengan melihat paket data yang dikirim dan diterima, Kita dapat mengidentifikasi masalah jaringan seperti kegagalan koneksi, latensi tinggi, atau paket yang hilang.

Wireshark dapat digunakan untuk mendeteksi ancaman keamanan jaringan. Kita dapat melihat aktivitas yang mencurigakan, percobaan penetrasi, atau serangan

jaringan lainnya. Ini dapat membantu Kita merespons cepat untuk mengatasi ancaman keamanan sebelum mereka menyebabkan kerusakan lebih lanjut.

Kita dapat menggunakan Wireshark untuk menganalisis lalu lintas web yang melintasi jaringan Kita. Ini dapat membantu dalam mendeteksi ancaman keamanan web, memeriksa kinerja situs web, dan mengidentifikasi permintaan atau tanggapan HTTP yang bermasalah.

1. Manfaat Bagi Penulis

Penulis dapat mengimplementasikan ilmu penegtahuan yang dimilikinya yang di dapat dari perkuliahan.

2. Manfaat Terhadap Lokasi Penelitian

Di harapkan dengan adanya penelitian ini, maka menjadi bahan referensi bagi lokasi yg di pakai untuk penelitian, agar dapat mengoptimalkan system keamanan jaringan dengan memanfaatkan *tools* bantuan seperti *wireshark* dalam memonitoring lalu lintas jaringan , yang juga dapat di gunakan untuk mengcapture hasil dari *Monitoring* paket data yang keluar dan masuk pada jaringan , Serta biasa memberikan gambaran sebuah system yang berjalan dengan baik, di tinjau dari segi keamanan jaringan itu sendiri.

3. Manfaat Terhadap Dunia Akademis

Penelitian Ini dapat di jadikan bahan atau *referensi* dalam penelitian selanjutnya tentang sistem keamanan jaringan Komputer.

## 1.5 Penelitian Terdahulu

Penelitian terdahulu merupakan upaya penelitian untuk mencari pembanding kemudian menemukan inspirasi baru untuk penelitian selanjutnya. Selain itu, Penelitian sebelumnya membantu mempromosikan penelitian dan menunjukkan *orisinalitas* penelitian.

1. Penelitian terdahulu ini di ambil dari jurnal yang di tulis oleh bapak Abdul Majid dan Bapak Timur Dali Purwanto, Pada penelitian ini penulis menggunakan sebuah metode action research, Metode action research ini memiliki beberapa tahapan yaitu.

1. Melakukan Diagnosa (*Diagnosing*)
2. Membuat rencana tindakan (*Action planning*)
3. Melakukan tindakan (*Action Tacking*)
4. Melakukan evaluasi (*Evaluating*)
5. Pembelajaran (*learning*)

2. Penelitian terdahulu ini di ambil dari jurnal yang di tulis oleh Yesi Febriani dan Vivi Sahfitri, Dalam penelitian ini penulis melakukan penelitian dengan menggunakan metode Action Research yang bertujuan untuk mengembangkan keterampilan-keterampilan baru atau cara-cara pendekatan baru dan untuk memecahkan masalah dengan cara penerapan langsung pada objek penelitian.



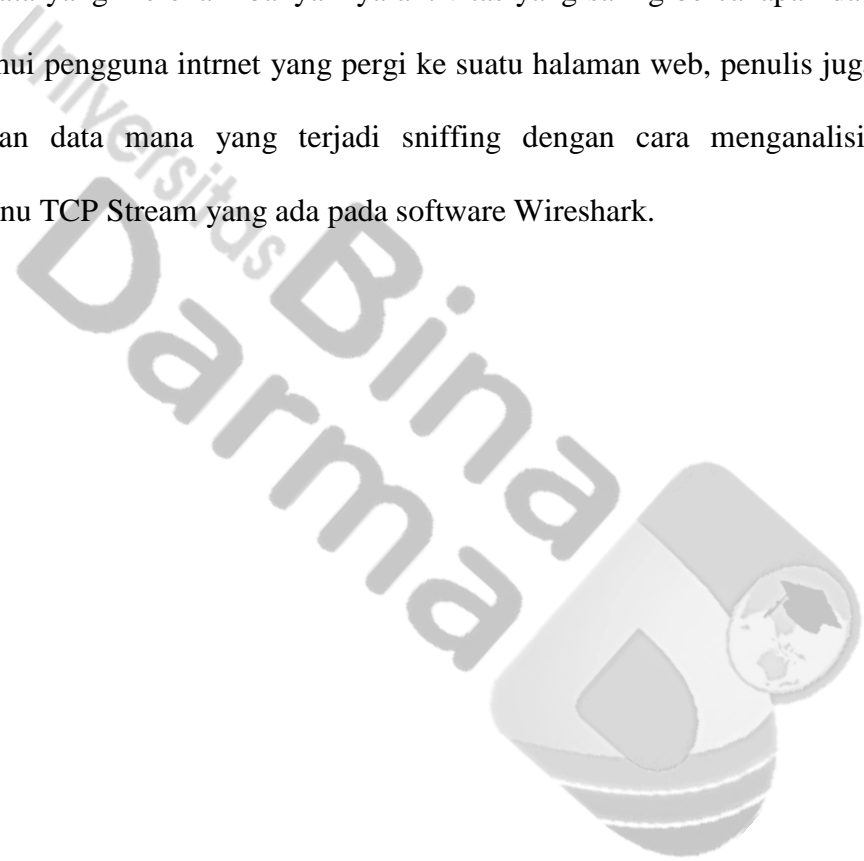
1. Melakukan Diagnosa (Diagnosing) Setelah melakukan magang pada Kantor Dinas ESDM Prov. Sumsel, peneliti melakukan diagnosa setelah melihat beberapa pegawai mencoba login pada halaman web yang belum tentu memiliki standar keamanan. Sehingga dapat memungkinkan bila informasi pribadi seperti password atau e-mail dapat terdeksi. Bila info penting seperti e-mail pengguna internet dapat terdeksi bahkan bila e-mail tersebut bersangkutan dengan banyak akun lainnya, itu dapat membahayakan lebih merugikan pengguna internet sehingga dapat disalah gunakan oleh orang lain.

2. Membuat Rencana Tindakan (Action Planning) Pada tahap ini penulis berencana membuat tindakan pada Kantor Dinas ESDM Sumatera Selatan, berikut ini rencana tindakan meliputi :

- 1) Memonitoring menggunakan dua software yaitu Wireshark dan Microsoft Network Monitor selama 14 hari dimulai pada tanggal 15 Maret sampai 30 Maret (terpotong hari minggu)
- 2) Menyimpan hasil rekaman traffic data setiap tanggalnya menggunakan Wireshark
- 3) Mengecek hasil rekaman membaca apakah terdapat sniffing atau tidak dengan cara melalui TCP Stream dan dilihat apakah traffic data terenkripsi atau tidak, dan mencari data penting pengguna internet
- 4) Membandingkan kedua software yang digunakan, manakah yang lebih baik
- 5) Menginformasikan bahwa ada data pengguna internet yang telah tersniffing.

3. Melakukan Evaluasi (Evaluating)

Peneliti melakukan evaluasi dan penarikan kesimpulan dari monitoring yang telah dilakukan pada Kantor Dinas ESDM Sumatera Selatan. Dapat dilihat dari hasil rekaman traffic data yang merekam banyaknya aktivitas yang saling bercakapan dan juga dapat diketahui pengguna intrnet yang pergi ke suatu halaman web, penulis juga membeda rekaman data mana yang terjadi sniffing dengan cara menganalisis menggunakan menu TCP Stream yang ada pada software Wireshark.



## BAB II

### METODOLOGI PENELITIAN

#### 2.1 Gambaran Objek Penelitian

##### 2.1.1 Profil Instansi

PT Pupuk Sriwijaya Palembang (Pusri) adalah perusahaan yang didirikan sebagai pelopor produsen pupuk urea di Indonesia pada tanggal 24 Desember 1959 di Palembang Sumatera Selatan, dengan nama PT Pupuk Sriwidjaya (Persero). Pusri memulai operasional usaha dengan tujuan utama untuk melaksanakan dan menunjang kebijaksanaan dan program pemerintah di bidang ekonomi dan pembangunan nasional. Sejarah panjang Pusri sebagai pelopor produsen pupuk nasional selama lebih dari 50 tahun telah membuktikan kemampuan dan komitmen dalam melaksanakan tugas penting yang di berikan oleh pemerintah.

Selain sebagai produsen pupuk nasional, Pusri juga mengemban tugas dalam melaksakan usaha perdagangan, bertanggung jawab dalam melaksanakan distribusi dan pemasaran pupuk bersubsidi kepada petani sebagai pelaksanaan *Public Service Obligation (PSO)* untuk mendukung program pangan nasional dengan memprioritaskan produksi dan pendistribusian public bagi petani di seluruh wilayah Indonesia. kebutuhan pupuk sektor perkebunan industri maupun ekspor menjadi bagian kegiatan perusahaan yang lainnya di luar tanggung jawab pelaksanaan *Public Service Obligation (PSO)*.

Sebagai Perusahaan yang bertanggung jawab atas kelangsungan pupuk nasional Pusri telah mengalami berbagai perubahan dalam manajemen dan wewenang yang sangat berkaitan dengan kebijakan-kebijakan pemerintah Sejak tanggal 18 April 2012, Kementerian BUMN meresmikan PT Pupuk Indonesia (Persero) sebagai nama induk perusahaan pupuk yang baru, menggantikan nama PT Pusri (Persero).

PT Pupuk Indonesia (Persero) merupakan pemegang saham utama dan pengendali Pusri dengan kepemilikan sebesar 99.9998%. Sementara entitas pemilik akhir dari pupuk Indonesia adalah Pemerintah Republik Indonesia yang memiliki seluruh (100.00%) saham PT Pupuk Indonesia (Persero). Hingga saat ini Pusri secara resmi beroperasi dengan nama PT Pupuk Sriwidjaja Palembang dan tetap menggunakan brand dan merek dagang Pusri.

### **2.1.2 Visi dan Misi Instansi**

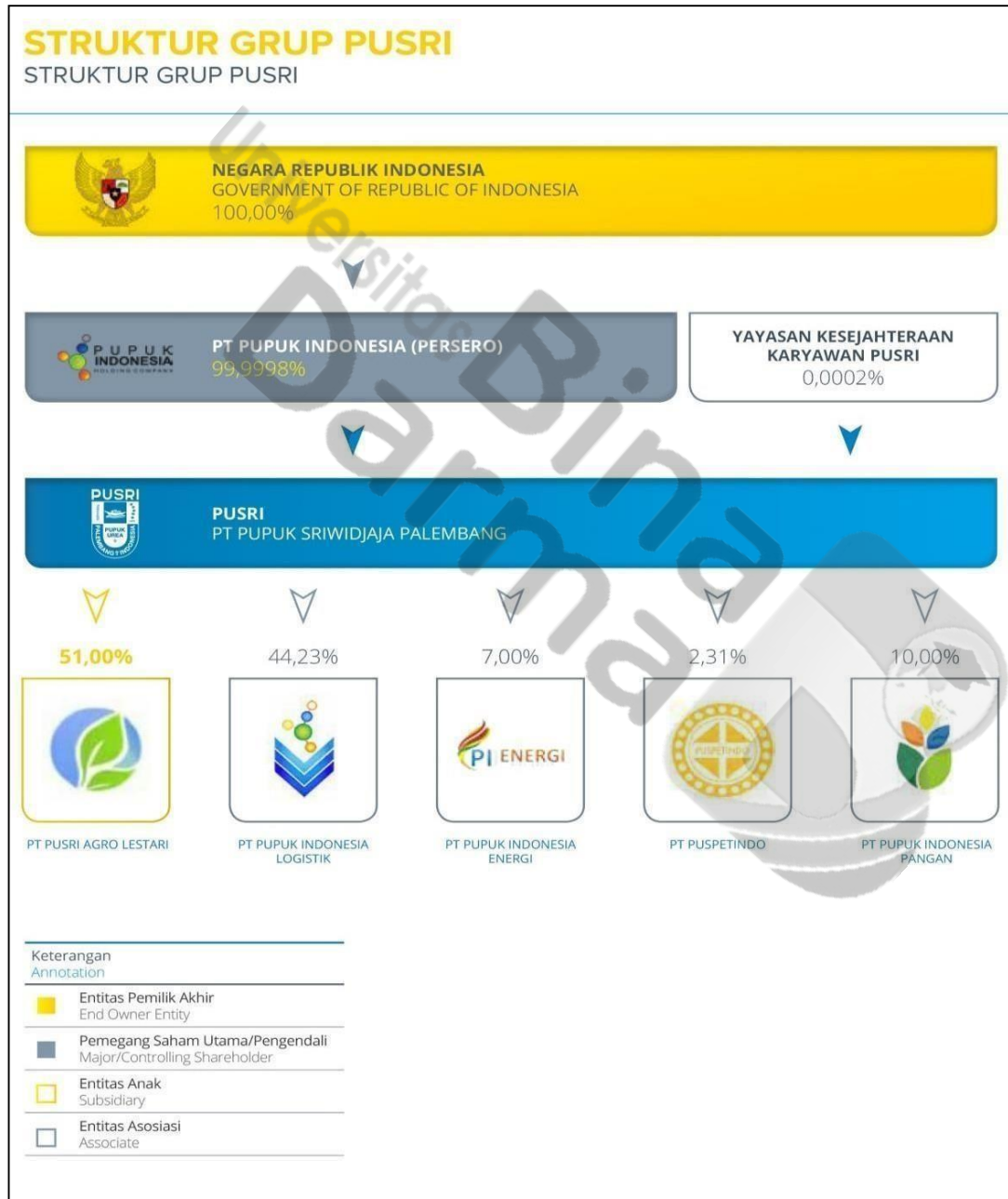
#### **1. Visi**

1. Menjadi Perusahaan *Agroindustri* Unggul di Asia

#### **2 Misi**

1. Menyediakan produk dan solusi *agroindustri* yang terintegrasi
2. Memberikan nilai tambah kepada *stakeholders* secara berkelanjutan
3. Mendukung pencapaian kemandirian pangan dan kemakmuran Negeri

### 2.1.3 Struktur Grup Instansi



**Gambar 2.1** Struktur Grup Pusri

#### 2.1.4 Makna Lambang

Kejayaan dan kemenangan yang gilang-gemilang mengabadikan masa kejayaan dan menentukan cita-cita besar yang harus di raih. Kerajaan maritime Sriwidjaja Sejarah telah mencatat bahwa di abad ke-7 telah berdiri sebuah kerajaan maritime yang sangat kuat yang bernama Sriwidjaja, Kerajaan ini memulai kekuasaannya di Pulau Sumatera dan terus membentangkan kekuatannya dari Sumatera ke Jawa, pesisir Kalimantan sampai Kamboja, Thailand Selatan, Semenanjung Malaya, Sebagian kawasan Indo China, dan telah melakukan perdagangan luas dengan India dan daratan Cina. Nama dan pengaruh kerajaan ini bahkan terdengar sampai ke penjuru dunia baik dalam kekuatan perdagangan, agama, budaya dan armadanya yang berjaya dan dapat menguasai kawasan samudra Hindia dan Pasifik.



Dalam Bahasa Sanskerta Sri mempunyai arti “bercahaya” atau “ gemilang”, dan Widjaja berarti “kemenangan” atau “ kejayaan “ Secara penuh nama Sriwidjaja mempunyai arti “kejayaan atau kemenangan yang Gilang-gemilang”. Kerajaan Bahari ini amat berkuasa dan berpengaruh dan di pimpin oleh raja-raja keturunan dinasti Syailendra, Pusat perniagaan kerajaan ini dulu di bangun di bukit Siguntang yang berdiri di muara dua sungai Musi yang kini di sebut Palembang, Sebuah kebanggaan yang sekaligus menjadi tolak ukur bagi segenap rakyat Indonesia khususnya masyarakat Palembang untuk mewarisi kebesaran sebuah sejarah.

### 2.1.5 Filosofi Nama Instansi




	<p><b>PT Pupuk Sriwidjaja Palembang</b></p> <p>Nama Sriwidjaja diabadikan di perusahaan ini untuk mengenang dan mengangkat kembali masa kejayaan kerajaan maritim pertama di Indonesia yang termahsyur di seluruh penjuru dunia. Sebuah penghormatan kepada leluhur yang pernah membuktikan bahwa Indonesia adalah bangsa yang besar. Pendirian pabrik pupuk dengan nama PT Pupuk Sriwidjaja Palembang, adalah warisan yang sekaligus menjadi visi bangsa Indonesia terhadap kekuatan, kesatuan, dan ketahanan wawasan Nusantara.</p>
---	---

*Gambar 2.2 Logo Pusri 1*

### 2.1.6 Detail Elemen Visual Logo instansi

NO	LOGO	KETERANGAN
1		Lambang Pusri yang berbentuk huruf "U" melambangkan singkatan "Urea". Lambang ini telah terdaftar di Ditjen Haki Dep. Kehakiman & HAM No. 021391
2		Setangkai padi dengan jumlah butiran 24 melambangkan tanggal akte pendirian PT Pusri.



3		<p>Butiran-butiran urea berwarna putih sejumlah 12, melambangkan bulan Desember pendirian PT Pusri.</p>
4		<p>Setangkai kapas yang mekar dari kelopaknya. Butir kapas yang mekar berjumlah 5 buah Kelopak yang pecah berbentuk 9 retakan ini, melambangkan angka 59 sebagai tahun pendirian PT Pusri (1959).</p>
5		<p>Perahu Kajang, merupakan legenda rakyat dan ciri khas kota Palembang yang terletak di tepian Sungai Musi. Perahu Kajang juga diangkat sebagai merk dagang PT Pupuk Sriwidjaja.</p>

6		Kuncup teratai yang akan mekar, merupakan imajinasi pencipta akan prospek perusahaan dimasa datang.
7		Komposisi warna lambang kuning dan biru benhur dengan dibatasi garis-garis hitam tipis (untuk lebih menjelaskan gambar) yang melambangkan keagungan, kebebasan cita-cita, serta kesuburan, ketenangan, dan ketabahan dalam mengejar dan mewujudkan cita-cita itu.

**Tabel 2. 1** Makna Logo Pusri

### 2.1.7 Identitas Instansi

Dalam bentuk komunikasi apapun, sangat penting bagi sebuah Perusahaan untuk menjaga konsistensinya, salah satunya adalah konsistensi terhadap identitasnya.

Identitas perusahaan atau jati diri perusahaan (*corporate identity*) adalah semua perwakilan atau perwujudan media visual dan fisik yang menampilkan suatu jati diri perusahaan sehingga dapat membedakan perusahaan tersebut dengan Perusahaan lainnya.

Dalam bidang *public relations*, relasi identitas Perusahaan dijelaskan dalam bentuk model dinamika identitas Perusahaan yang dikemukakan oleh *Hacth and Schultz* . Model dinamika tersebut menyebutkan bahwa identitas Perusahaan memiliki

relasi dengan budaya perusahaan (*corporate culture*) dan citra perusahaan (*corporate image*). Secara internal, identitas Perusahaan terkait dengan kultur / budaya yang dianut oleh Perusahaan. Namun, secara eksternal, identitas Perusahaan memiliki keterkaitan dengan citra perusahaan. Saat ini, identitas Perusahaan telah diakui sebagai sumber daya yang strategis dan sumber keunggulan yang kompetitif.

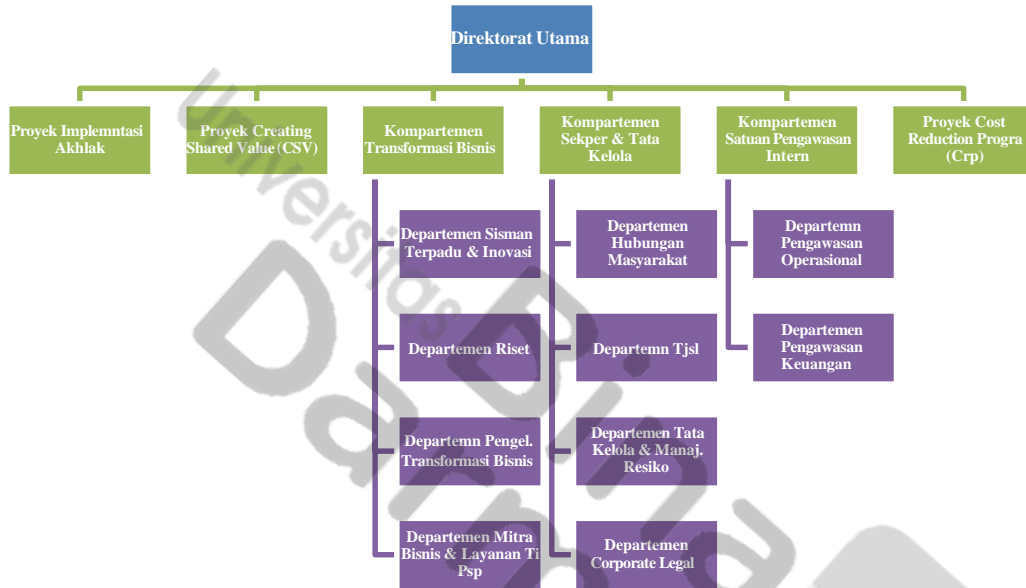
Keseragaman persepsi dalam penerapan logo, warna, dan tipografi yang konsisten sangatlah penting jika ingin menjaga kehadiran brand yang kuat di pasaran. Dan yang paling penting adalah kesatuan semangat semua pihak yang berkepentingan baik di dalam maupun di luar lingkungan PT Pusri Palembang untuk mencapai tujuan bersama yaitu menjadikan PT Pusri Palembang menjadi perusahaan besar yang berperan aktif dalam mewujudkan Indonesia yang makmur dan berkeadilan pangan.

PT Pupuk Sriwidjaja Palembang (Pusri) adalah perusahaan yang didirikan sebagai pelopor produsen pupuk urea di Indonesia pada tanggal 24 Desember 1959 di Palembang Sumatera Selatan, dengan nama PT Pupuk Sriwidjaja Palembang (Persero). Pusri memulai operasional usaha dengan tujuan utama untuk melaksanakan dan menunjang kebijaksanaan dan program pemerintah di bidang ekonomi dan pembangunan nasional, khususnya di industri pupuk dan kimia lainnya. Sejarah panjang pusri sebagai pelopor produsen pupuk nasional selama lebih dari 50 tahun telah membuktikan kemampuan dan komitmen kami dalam melaksanakan tugas penting yang di berikan oleh pemerintah.

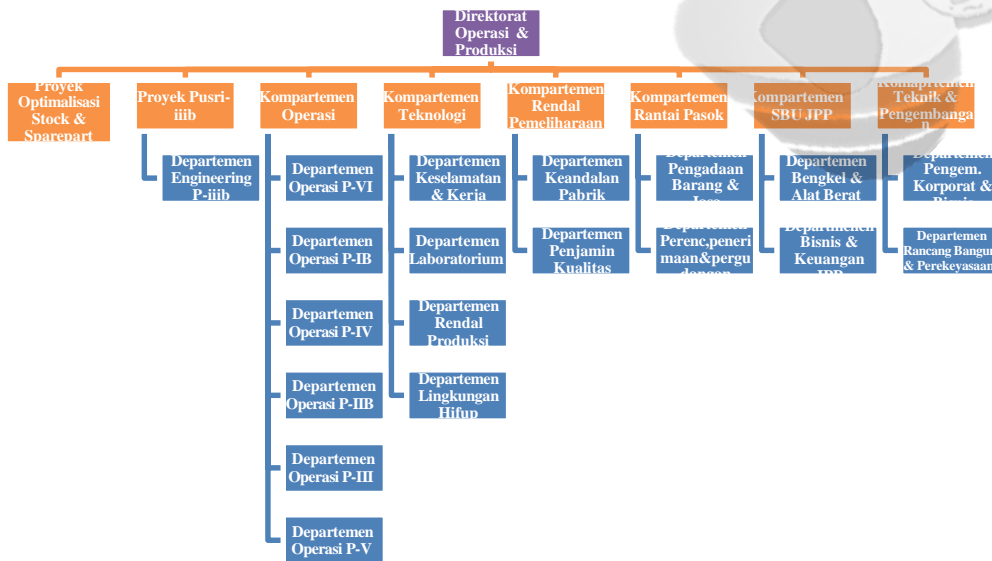
### **2.1.8 Struktur Organisasi PT Pusri Palembang**

Struktur organisasi merupakan bagian yang tidak terpisahkan di dalam suatu organisasi, badan usaha, ataupun instansi. Setiap instansi mempunyai struktur organisasi yang berbeda. Penyusunan struktur organisasi merupakan langkah awal dalam memulai pelaksanaan kegiatan perusahaan, dengan kata lain penyusunan struktur organisasi adalah langkah terencana dalam suatu perusahaan untuk melaksanakan fungsi perencanaan, pengorganisasian, pengarahan, dan pengawasan. Menurut Robbins dan Coulter, struktur organisasi dapat diartikan sebagai kerangka kerja formal organisasi yang dengan kerangka kerja itu tugas-tugas pekerjaan dibagi, dikelompokkan, dan dikoordinasikan. Struktur organisasi dapat menghindari atau mengurangi kesimpangsiuran dalam pelaksanaan tugas.

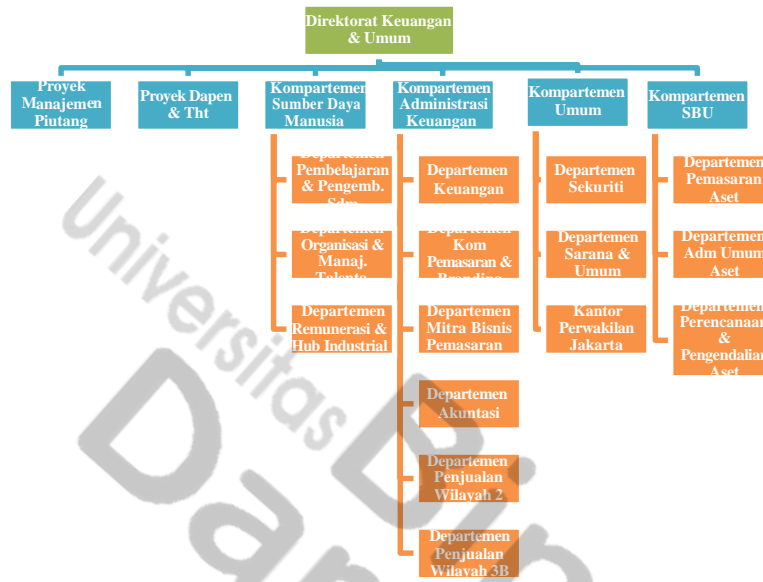
## Bagan Struktur Organisasi PT Pupuk Sriwidjaja Palembang



Gambar 2.3 Struktur Organisasi PT. Pusri 1



Gambar 2.4 Struktur Organisasi PT. Pusri 1

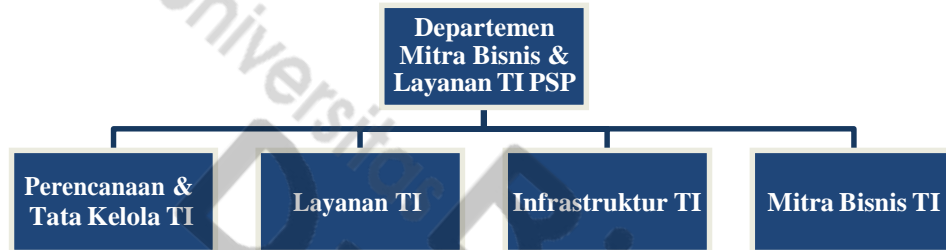


Gambar 2.5 Struktur Organisasi PT.Pusri. 1

### 2.1.9 Sistem Manajemen dan Struktur Organisasi Departemen Mitra Bisnis dan Layanan TI PSP

Departemen Teknologi Informasi dipimpin oleh seorang Manajer yang membawahi Staf Senior Perencanaan dan Penunjang Teknologi Informasi beserta Staf, Superintendent Pengembangan Sistem Informasi Kantor Pusat dan Kantor Produksi beserta Staf, Superintendent Pengembangan Sistem Informasi Pemasaran dan Unit Penunjang beserta Staf, Superintendent Pengoperasian Sistem Komputer beserta Staf, dan Superintendent Pemeliharaan Komputer dan Komunikasi Data Beserta Staf.

## Bagan Struktur Organisasi Departemen Mitra Bisnis dan Layanan TI PSP



*Gambar 2.6 Struktur Departemen Mitra B I*

### **2.2 Monitoring**

Monitoring merupakan aktivitas mengumpulkan dan menganalisis data berdasarkan faktor yang ditetapkan secara teratur kemudian berlanjut pada aktivitas program sehingga bisa melakukan tindakan koreksi untuk menyempurnakan aktivitas program tersebut

### **2.3 Analisis**

Analisis adalah kegiatan untuk mencari pola, atau cara berpikir yang berkaitan dengan pengujian secara sistematis terhadap sesuatu untuk menentukan bagian, hubungan antar bagian, serta hubungannya dengan keseluruhan.

## **2.4 Pengertian mencegah**

Menurut Kamus Besar Bahasa Indonesia (KBBI), kata mencegah /me•cegaH/ dapat didefinisikan sebagai berikut.

- 1) Mengikhtiarkan supaya jangan terjadi
- 2) Merintang; melarang
- 3) Menahan agar sesuatu tidak terjadi; menegahkan; tidak menurutkan

## **2.5 Wireless**

Wireless atau yang dikenal dengan jaringan nirkabel wireless atau wireless Network merupakan sekumpulan komputer yang saling terhubung antara satu dengan lainnya sehingga terbentuk sebuah jaringan komputer dengan menggunakan media udara/gelombang sebagai jalur lintas datanya. Teknologi wireless adalah salah satu pilihan yang tepat untuk menggantikan teknologi jaringan yang terdiri dari banyak kabel dan merupakan sebuah solusi akibat jarak antar jaringan yang tidak mungkin dihubungkan melalui kabel. Keuntungan terbesar dari wireless yaitu sangat praktis, dimana komputer dapat terhubung ke jaringan tanpa membutuhkan kabel.

## **2.6 Web Traffic**

Traffic pada website merupakan jumlah orang yang mengunjungi website, membuka halaman website, dan durasi saat pengunjung membuka dan membaca



halaman pada website kamu. Jadi, saat seseorang mengunjungi website kamu, kunjungan serta semua link yang mereka klik dan follow akan direkam oleh domain kamu. Nantinya angka-angka akan memberi ide tentang seberapa populernya website kamu.

### **2.7 Cyber Crime**

Cyber Crime merupakan aktivitas individu maupun kelompok yang mengguakan jaringan komputer sebagai media untuk melakukan tindakan kriminal, atau menjadikan komputer sebagai sasaran kejahatan

### **2.8 Jaringan Komputer**

Jaringan Komputer merupakan hubungan dengan beberapa perangkat yang bisa saling berkomunikasi satu sama lain. Perangkat yang dimaksud pada definisi ini mencakup komputer desktop, samrthphone, tablet, router, switch, dan hub

### **2.9 Keamanan Jaringan**

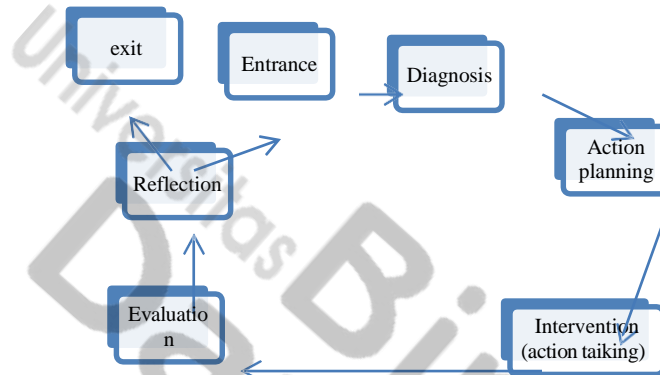
Keamanan jaringan yang terkendalnya atas akses penggunaan jaringannya dimana seseorang dapat mengakses jaringan dan dikendalikan oleh siapapun yang berhak juga bisa menghalangi subjek maupun orang asing yang tidak memiliki hak untuk masuk ke dalam jaringan.

### **2.10 Wireshark**

Wireshark merupakan tool yang ditunjukkan untuk menganalisa paket data jaringan, Wireshark juga disebut Network Packet Analyzer yang memiliki fungsi untuk menangkap paket data dalam jaringan dan berusaha memperlihatkan informasi dipaket tersebut secara rinci.

## 2.11 Metode Penelitian

Dalam penelitian kali ini penulis menggunakan metode *Action Research*.



Gambar 2.7 Metode Action Research I

Davison, et al (2004) Metode *Reaction Research* ini di bertujuan untuk pengujian dan pengembangan, menemukan dan merancang, langkah-langkah ini diterapkan di tempat kerja (Objek), Dengan menggunakan metode ini pekerjaan akan menjadi lebih muda, lebih cepat dan hasilnya lebih baik dan lenih berkualitas.

### 2.11.1 Diagnose (Diagnosis)

Setelah melaksanakan magang di PT Pupuk Sriwidjaja Palembang, Peneliti Melakukan diagnosis setelah melihat beberapa karyawan mencoba masuk ke situs *web* yang mungkin belum memiliki standar keamanan, sehingga informasi pribadi seperti *Password* atau *email* dapat di kenali, Jika informasi penting seperti alamat email pengguna internet dapat di dideteksi meskipun email tersebut di tautkan ke banyak

akun lain, ini dapat lebih berbahaya bagi pengguna unternet dan memungkinkan orang lain untuk menyalahgunakan.

## **2.11.2 Alat Alat yang Digunakan Topologi Pada PT. Pupuk Srwiridjaja**

### **a. Router**

Router merupakan salah satu komponen pada jaringan komputer yang mampu melewati data melalui sebuah jaringan atau internet menuju sasaran, melalui sebuah proses yang di kenal sebagai routing, Router berfungsi sebagai penghubung antar 2 (dua) atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya (Mhd. Dicky Syahpura LUBIS, dkk, 2020).

### **b. Proxy**

Proxy adalah sistem yang menengahi pengguna dan internet untuk menyembunyikan identitas asli pengguna, sehingga data yang dikirim ke website tujuan akan menggunakan alamat IP dari proxy server, bukan alamat IP pengguna. (HeruKurniawan, dkk, 2020).

### **c. Hub**

Hub adalah perangkat jaringan yang memungkinkan Anda menghubungkan beberapa PC ke satu jaringan. Perangkat ini digunakan untuk menghubungkan segmen LAN. Sebuah hub memiliki berbagai macam port, jadi

ketika sebuah paket tiba di satu port, itu disalin ke berbagai port lainnya. (Rizky Amanda, dkk, 2020).

#### **d. Switch**

switch adalah sebuah komponen jaringan yang tugasnya untuk menghubungkan beberapa perangkat, untuk bisa melakukan pertukaran paket data, baik dalam proses penerimaan, serta meneruskan data ke perangkat lain.(Desmira, dkk, 2020).

#### **e. Kabel UTP**

UTP merupakan singkatan dari Unshield Twisted Pair. Sesuai namanya “Unshield”, yang berarti kabel ini tidak dilengkapi dengan pelindung aluminium sehingga jenis kabel ini kurang tahan dengan interferensi elektromagnetik, berbeda dengan saudaranya STP (Shield Twisted Pair).(Bobi Agustian, Muhammad Yasser Arafat,2020).

#### **f. Kabel Fiber Optic**

Fiber Optik adalah saluran transmisi atau sejenis kabel yang terbuat dari kaca atau plastik yang sangat halus dan lebih kecil dari sehelai rambut, dan dapat digunakan untuk mentransmisikan sinyal cahaya dari suatu tempat ke tempat lain. Sumber cahaya yang digunakan biasanya adalah laser atau LED.(Amalia Rizqi Utami, dkk, 2020).

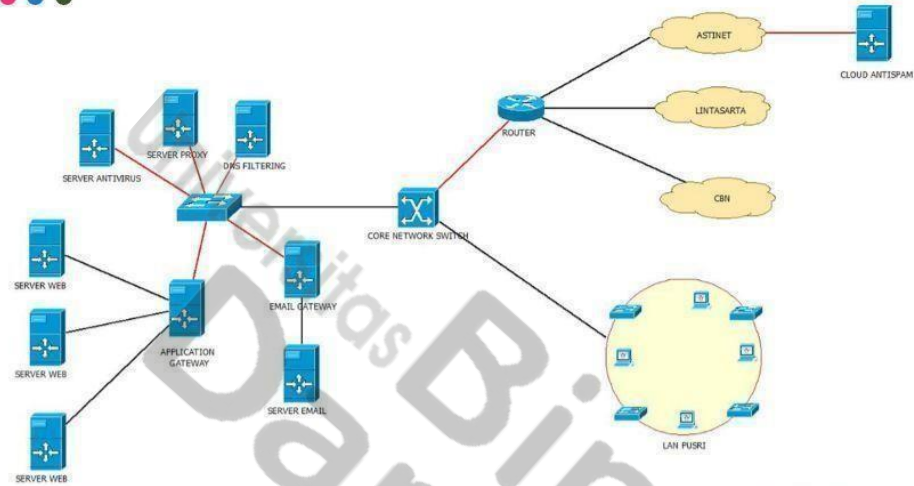
### **g. Kabel Koaksil**

Kabel coaxial merupakan kabel yang mempunyai 2 konduktor yakni copper pada bagian tengahnya atau pusat inti yang terbuat dari tembaga bertekstur keras dan dilapisi dengan isolator. Sementara konduktor kedua adalah yang melingkar pada bagian luar isolator pertama serta tertutup dengan insulator luar. (Anisa Yulia Haryanti, dkk, 2021)

#### **2.11.3 Topologi Jaringan PT.Pupuk Sriwidjaja Palembang**

Topologi jaringan pada PT. Pupuk Sriwidjaja Palembang banyak menggunakan tipe topologi star, tetapi ada juga yang menggunakan topologi bus dan topologi tree. Topologi star merupakan topologi jaringan yang menggunakan concentrator (hub/switch) untuk mengatur paket data. Topologi ini memiliki kontrol terpusat. Semua link harus melewati pusat yang menyalurkan data ke semua simpul (client) , simpul pusat disebut simpul stasiun primer (server), simpul lain disebut stasiun sekunder (client server) (Lalu Deisi Samsumar dan Moh. Subli 2019). Berikut adalah gambar Topologi Jaringan Star pada PT. Pupuk Sriwidjaja Palembang :

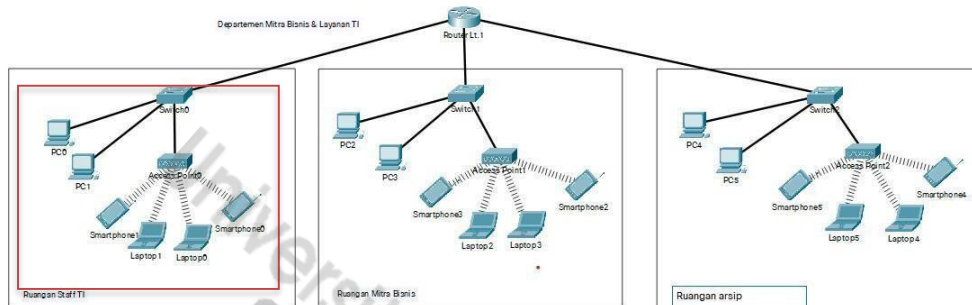
# Network Topology



PT Pusri Palembang

Gambar 2.8 Topologi Jaringan PT.Pusri 1

### 2.11.4 Topologi jaringan departemen TI



Gambar 2.9 Topologi Departement TI

Pada gambar 2.9 departemen TI memiliki tiga ruangan dengan masing-masing memiliki jaringan tersendiri dimana pada penelitian ini saya melakukan monitoring lalu lintas jaringan pada ruangan staff TI dengan nama jaringan Wifi PUSRI.NET .

### 2.11.5 Rencana Tindakan (Action Planing)

Saat ini Penulis melakukan magang di PT Pupuk Sriwidjaja Palembang,

Rencana aksi berikut meliputi:

1. Melakukan *Monitoring* dengan satu program yaitu *Wireshark* selama dua minggu atau 16 hari dari tanggal 6 juni sampai 22 juni ( Kecuali sabtu Minggu dan hari libur ).
2. Pencatatan lalu lintas harian dengan menggunakan *wireshark*.
3. Memeriksa log baca untuk mengendus atau tidak melewati aliran *TCP* lihat apakah lalu lintas dienkripsi atau tidak dan cari informasi penting dari pengguna internet.

4. Perbandingan dua program bekas mana yang lebih baik.
5. Diberitahu bahwa pengguna internet difilter menurut orang lain.

#### **2.11.5 Evaluasi (Evaluating)**

Penelitian melakukan evaluasi dan menarik kesimpulan dari pemantauan yang dilakukan di PT Pupuk Sriwidjaja Palembang, Selain itu dari hasil perekaman data lalu lintas yang mencatat jumlah aktivitas komunikasi dan juga terlihat oleh pengguna internet yang mengunjungi situs tersebut, penulis membedakan kumpulan data mana yang dimata-matai untuk dianalisis melalui menu *TCP* dari perangkat lunak *Wireshark*

#### **2.12 Rancangan Penelitian**

Rancangan penelitian adalah rencana umum penelitian yang mencakup pekerjaan yang dilakukan oleh peneliti mulai dari pembentukan hipotesis dan implikasi operasionalnya hingga analisis akhir bahan dari mana keputusan dibuat dan proposal dibuat, Berikut ini adalah rancangan peneliti :

1. Pengumpulan Data : Untuk penelitian ini kami membangun lingkungan jaringan yang direplikasi kami menggunakan perangkat lunak *wireshark*, untuk merekam lalu lintas jaringan di area tersebut , Data yang disimoan termasuk paket data yang dikirim antara perangkat yang berbeda di jaringan.
2. Analisis Data : Setelah pengumpulan data, kami menganalisis paket data yang ditangkap menggunakan *Wireshark*. Kami menganalisis jenis paket, alamat sumber dan tujuan protokol yang digunakan dan atribut terkait lainnya, Analisis ini



memberikan pemahaman yang lebih dalam tentang lalu lintas jaringan dan dapat membantu mengidentifikasi masalah keamanan, kinerja atau konfigurasi jaringan

3. Identifikasi Masalah dan Solusi : Berdasarkan hasil analisis, kami akan mengidentifikasi masalah yang ada di jaringan dan mencari solusi yang tepat. Misalnya, jika kami menemukan paket yang mencurigakan atau aktivitas yang tidak diinginkan, kami akan mengevaluasi praktik keamanan jaringan dan merekomendasikan tindakan.
4. Validasi : Kami memvalidasi hasil analisis dan solusi yang diusulkan dengan mengimplementasikan perubahan di lingkungan jaringan. Kami memantau dampak perubahan dan memeriksa apakah masalah yang teridentifikasi telah diselesaikan.
5. Evaluasi : Di sini kami mengevaluasi efektivitas penggunaan *Wireshark* sebagai alat pemantauan jaringan. Kami melihat keuntungan dan keterbatasan penggunaan *Wireshark* dan membuat rekomendasi untuk perbaikan dan pengembangan lebih lanjut.

Kesimpulan : Penelitian ini harus mengarah pada pemahaman yang lebih baik tentang lalu lintas jaringan dan membantu mengidentifikasi masalah dan menemukan solusi yang tepat. Menggunakan *Wireshark* sebagai alat analisis dan pemantauan jaringan telah terbukti efektif dan dapat memberikan informasi berharga kepada *administrator* jaringan. Dengan demikian, penelitian ini dapat berkontribusi pada pengembangan keamanan dan kinerja jaringan.

## **BAB III**

### **HASIL DAN PEMBAHASAN**

#### **3.1 Hasil**

Dalam Penelitian kali ini, Peneliti memonitoring jaringan Pada Departemen TI PT. Pupuk Sriwidjaja di mulai pada pukul 08.00 WIB sampai pukul 16.00 WIB dengan menggunakan software Wireshark versi 4.0.4 64bit, Berikut ini adalah hasil rangkuman dari pengecekan rekaman traffic data menggunakan Wireshark.

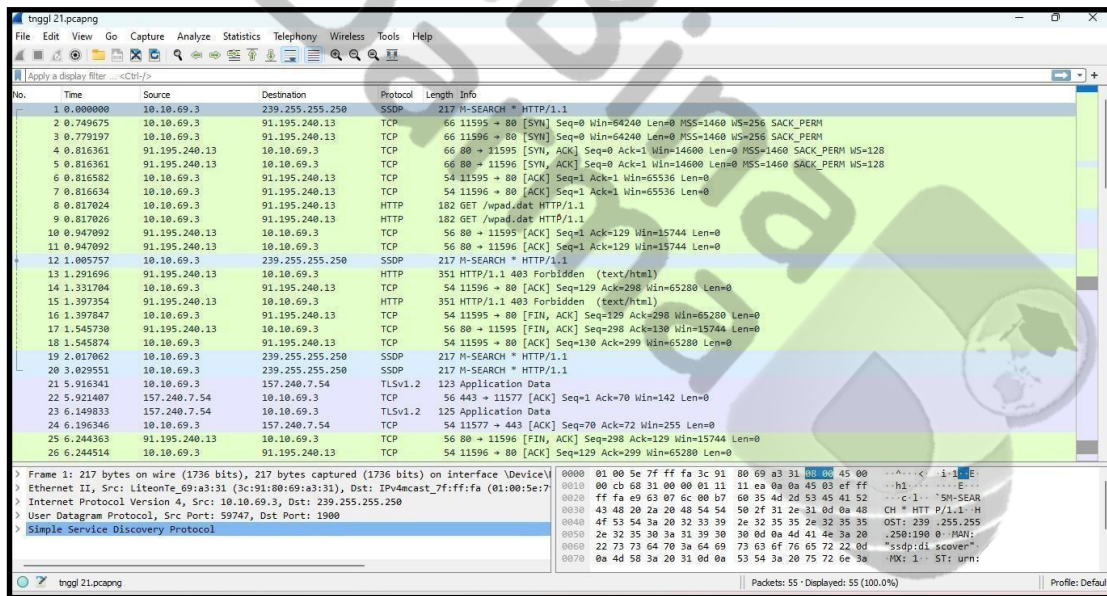
##### **3.1.1 Hasil Monitoring Wireshark**

Berikut ini adalah proses dan hasil dari monitoring jaringan menggunakan Wireshark di sertakan dengan analisis dengan menggunakan *TCP stream*.

### 3.1.2 Filtering Protokol HTTP

Disini penulis akan mmelakukan filtering paket data yang melewati protokol http pada beberapa jaringan yang ada di PT.Pupuk Sriwidjaja Palembang, selanjutnya ketikkan http pada kolom address filter.

#### 1. capturing filtering pada jaringan pusri.id new

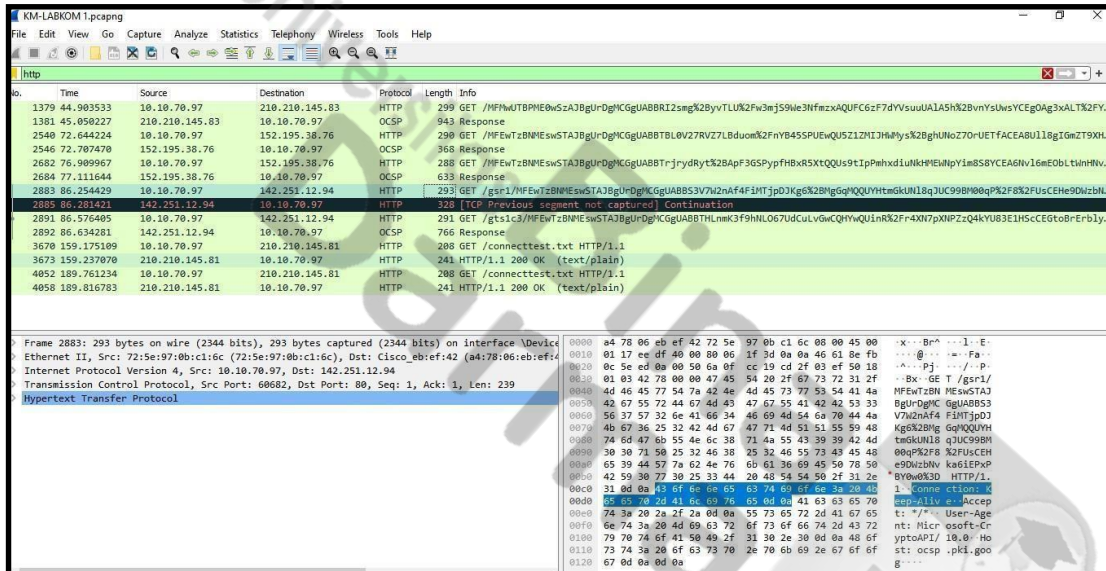


**Gambar 3. 1** filtering protokol http pada jaringan pusri.id new

Bisa di analisis user-agent yang di pakai pada jaringan Pusri.id New menggunakan Mozilla/5.0 (windows NT 10.0; WIN 64; x64) AppleWebKit/537.36 (KHTML, Like gecko) Chrome/115.0.0.0 Safari /537/36 Dan Host mysql - phi - intergration.com, Selain itu dapat di ketahui date yaitu 22 juni 2023 01:32 41 GMT DAN Full Request Get Uri Http, Disini bisa di lihat bahwa adanya aktivitas yang

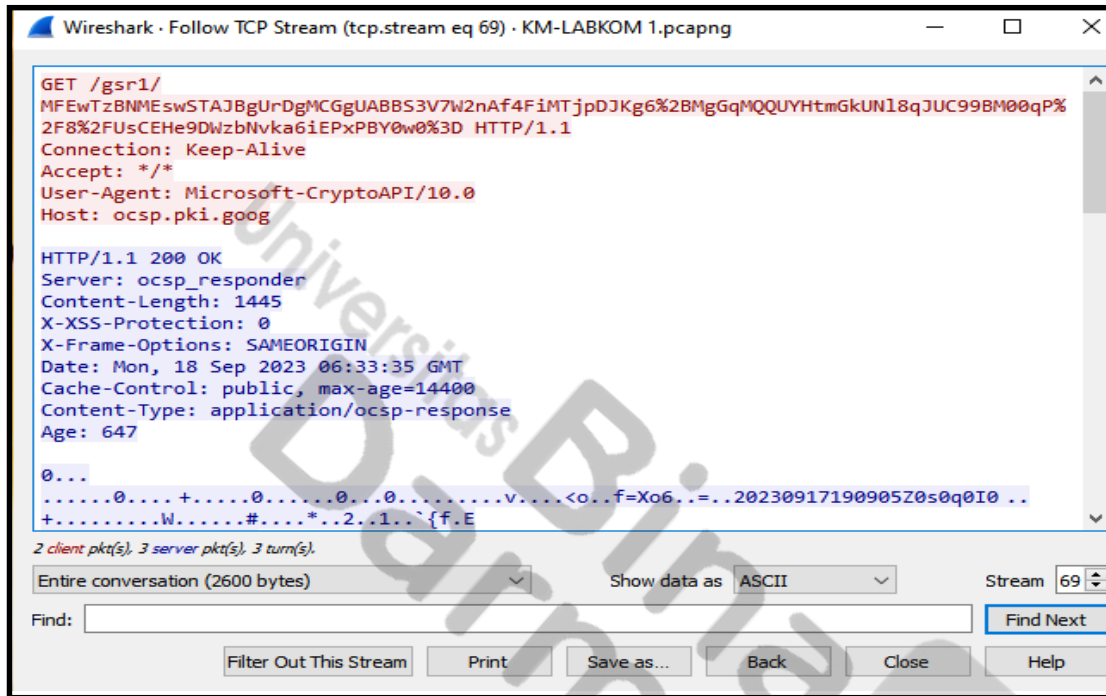
sedang mengakses laman web Gambar Capture TCP Stream Wireshark dibawah ini dapat melihat info get yang sedang di buka

## 2. Filtering protokol http pada jaringan KM-LABKOM



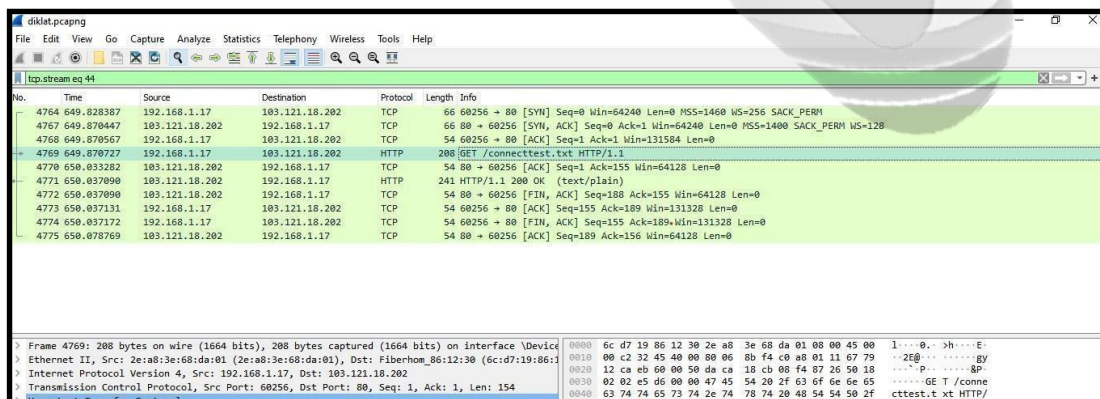
Gambar 3. 2 filtering protokol http pada jaringan KM-LABKOM

Bisa di analisis user-agent yang di pakai pada jaringan KM LABKOM menggunakan GET/gsr1/MFEwTzBNMEswSTA3BgUrDgMCGgUABBS3V7W2nAf4FiMTjpDJKg6%2BMgGqMQQUYHtmGkUNl8qJUC99BM00qP%2F8%2FUscEHe9DwzbnVka6iEPxPBY0w0%3D HTTP/1.1 Connection: Keep-Alive Accept: /\*/\* User-Agent: Microsoft-CryptoAPI/10.0 Host: ocs.pki.goog Selain itu dapat di ketahui date yaitu 18 September 2023 01:32 41 GMT DAN Full Request Get Uri Http, Disini bisa di lihat bahwa adanya aktivitas yang sedang mengakses laman web Gambar Capture TCP Stream Wireshark dibawah ini dapat melihat info get yang sedang di buka



Gambar 3.3 Tcp Stream

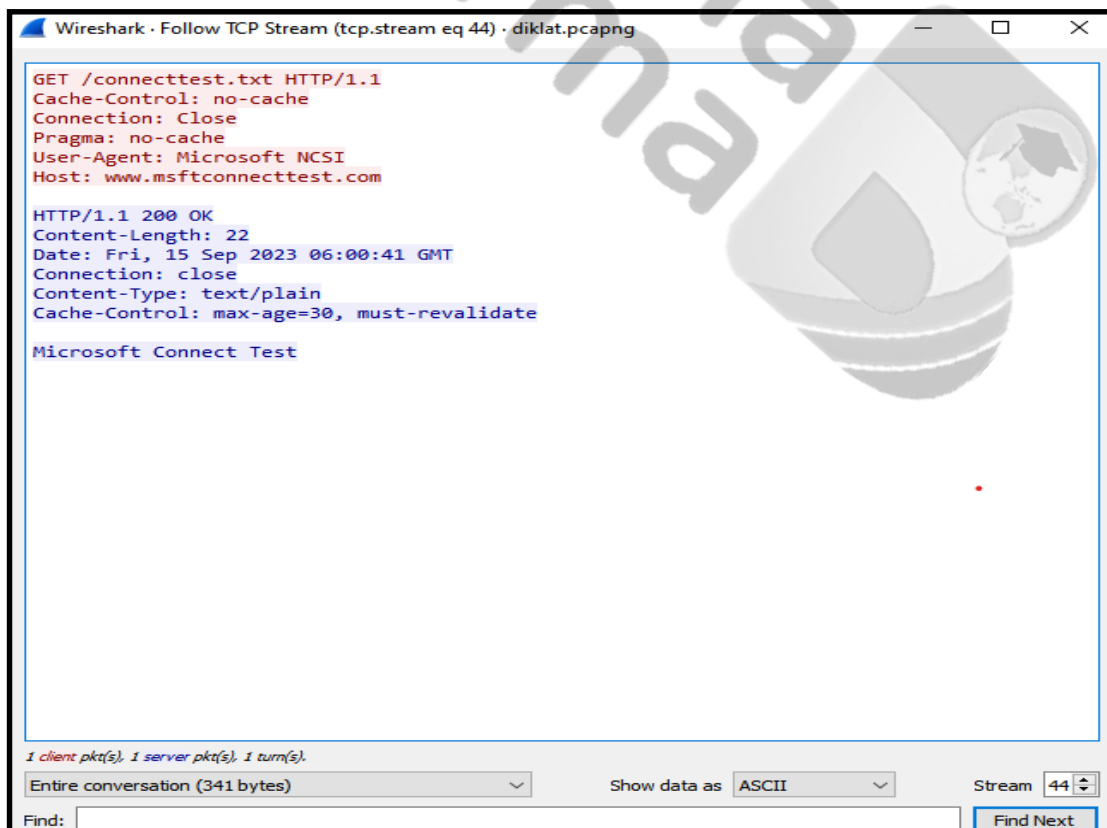
3. Filtering protokol http pada jaringan diklat.



Gambar 3.4 filtering protokol http pada jaringan diklat

Bisa di analisis user-agent yang di pakai pada jaringan Diklat GET /connecttest.txt HTTP/1.1 Cache-Control: no-cache Connection: Close Pragma: no-cache User-Agent: Microsoft NCSI Host:www.msftconnecttest.com,

Selain itu dapat di ketahui date yaitu HTTP/1.1 200 OK Content-Length: 22 Date: Fri, 15 Sep 2023 06:00:41 GMT Connection: close Content-Type: text/plain Cache-Control: max-age=30, must-revalidate Microsoft Connect TestDisini bisa di lihat bahwa adanya aktivitas yang sedang mengakses laman web Gambar Capture TCP Stream Wireshark dibawah ini dapat melihat info get yang sedang di buka



```
Wireshark · Follow TCP Stream (tcp.stream eq 44) · diklat.pcapng

GET /connecttest.txt HTTP/1.1
Cache-Control: no-cache
Connection: Close
Pragma: no-cache
User-Agent: Microsoft NCSI
Host: www.msftconnecttest.com

HTTP/1.1 200 OK
Content-Length: 22
Date: Fri, 15 Sep 2023 06:00:41 GMT
Connection: close
Content-Type: text/plain
Cache-Control: max-age=30, must-revalidate

Microsoft Connect Test
```

1 client pkt(s), 1 server pkt(s), 1 turn(s).

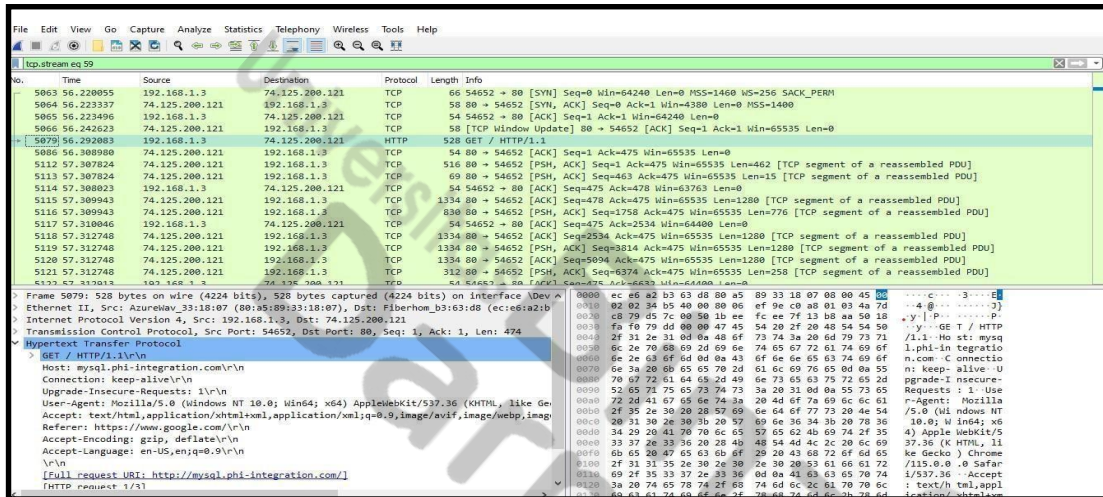
Entire conversation (341 bytes) Show data as ASCII Stream 44

Find: Find Next

**Gambar 3.5** tcp Stream



Pertukaran pada data-data di atas bisa di lihat dari gambar di bawah ini sedang melakukan pertukaran komunikasi data



Gambar 3. 6 Pertukaran Data

### 3.2 Analisis

Setelah melakukan filetring berikutnya dilakukan analisis paket data yang melewati protokol HTTP yang berisikan data post atau get yang terdapat informasi-informasi mengenai akses aktivitas jaringan yang dilakukan perangkat yang beralamat ip

#### 1. Analisis situs yang di akses dalam wireshark

- a. paket – paket data dari situs yang telah diakses tadi akana tercapture dan sidah di lakukan filtering
- b. Berikutnya pilihh dari paket – paket yang mengirimkan pesan Get lalu paketnya akan tercapture maka terlihat situs apa yag sedang di buka.

c. Contoh satu dalam Protokol http. Dalam Box Http terlihat permintaan source dan destination Src 152.195.38.76 Dst 10.10.70.97 HTTP 487GET Myqsl.phi-intergration.com/HTTP/1.1

2. Bisa di analisis user-agent yang di pakai pada jaringan Pusri.id New menggunakan Mozilla/5.0 (windows NT 10.0; WIN 64; x64) AppleWebKit/537.36 (KHTML, Like gecko) Chrome/115.0.0.0 Safari /537/36 Dan Host mysql - phi – intergration.com, Selain itu dapat di ketahui date yaitu 22 juni 2023 01:32 41 GMT DAN Full Request Get Uri Http, Disini bisa di lihat bahwa adanya aktivitas yang sedang mengakses laman web Gambar Capture TCP Stream Wireshark dibawah ini dapat melihat info get yang sedang di buka

```
GET / HTTP/1.1
Host: mysql.phi-integration.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
X-Robots-Tag: noarchive
Last-Modified: Wed, 02 Aug 2023 21:51:46 GMT
ETag: "1691013106000|#public|0|en|||0|995824666|555561292"
Expires: Wed, 16 Aug 2023 08:42:19 GMT
Date: Wed, 16 Aug 2023 08:42:19 GMT
Cache-Control: private, max-age=5
Content-Encoding: gzip
Transfer-Encoding: chunked
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Server: GSE
```

**Gambar 3. 7** TCP Stream



3. Bisa kita analisis yakni User –agent yang di pakai yaitu User- agent Mozilla/5.0 (Windows, NT 10,0 win64; x64 x64; rv:90.0) Gecko/201000-101 Browser yang di gunakan Chrome/115.0.0.0 Safari/537.36

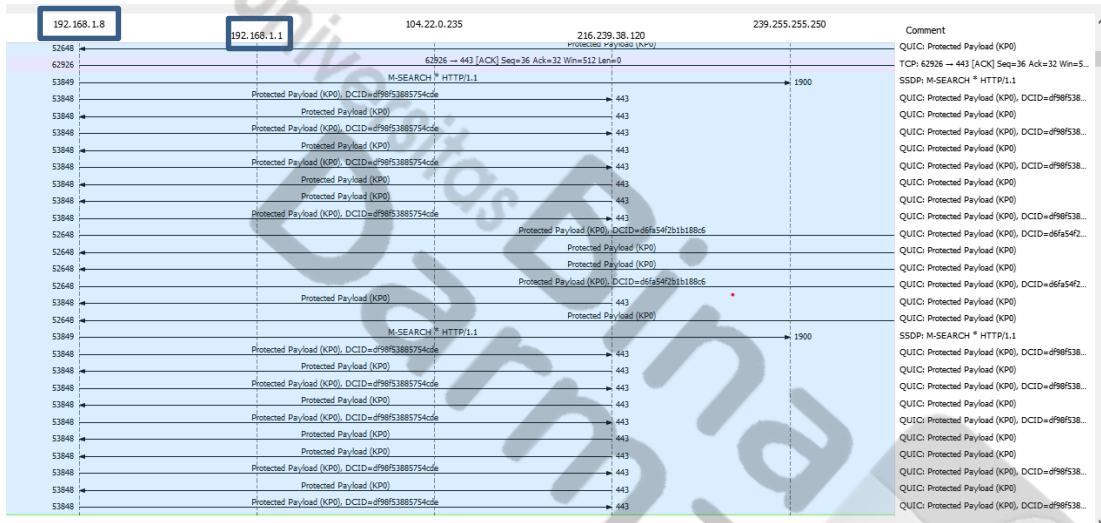
**Tabel 3. 1** Website yang di akses pengguna pada jaringan PT.Pusri

<b>NO</b>	<b>Website Yang Di Akses</b>	<b>Jenis Brwoser</b>
<b>1</b>	http://mysql-phi-integration	Google Mozila
<b>2</b>	Blog.spot.com	Google Mozila
<b>3</b>	www.msftconnecttest.com,	Google Mozila
<b>4</b>	ocsp,pki.goog	Google Mozila

**Tabel 3. 2** data ip akses protocol http

<b>TIME</b>	<b>SOURCE</b>	<b>DESTNATION</b>	<b>PROTOCOL</b>
0.069188	10.10.69.3	91.195.240.13	HTTP
650.037090	103.121.18.202	192.168.11.17	HTTP
86.281421	10.10.70.97	142.251.12.94	HTTP
72.863219	10.10.69.3	204.79.197.203	HTTP

Untuk melihat proses komunikasi data pada saat korban mengakses *Websit* Google Accounts dapat dilakukan dengan cara mengklik “*statistic*” pada menu bar kemudian pilih “*flow graph*” di bawah ini adalah tampilannya.



**Gambar 3. 8** Proses Komunikasi Data 1

Gambar 3.23 menunjukkan proses komunikasi data antar client yang memiliki ip address 192.168.1.8 Sedangkan server yaitu account google.com memiliki IP address 192.168.1.1

### 3.2 Pembahasan

Dapat di lihat dari hasil monitoring jaringan pada PT. Pupuk Sriwidjaja Palembang dengan menggunakan wireshark adanya 4 akses Protocol Http (Hypertext Transfer – Transfer Protocol). Dimana 4 akses tersebut di monitring dengan jaringan yang berbeda.

## BAB IV

### KESIMPULAN DAN SARAN

#### 4.1 Kesimpulan

Adapun penelitian pada jaringan di Departement TI PT. Pupuk Sriwidjaja Palembang adalah sebagai berikut.

1. Jaringan pada Departement TI PT. Pupuk Srwidjaja Palembang sudah cukup aman di karenakan pada saat di lakukannya monitoring jaringan tidak ada terjadinya akses illegal.
2. Wireshark memiliki keunggulan pada bagian *sniffing* di bandingkan software monitoring lainnya dan wiresahrk juga dapat membaca hasil *capture* dari *software monitoring* lainnya.
3. Wireshark adalah sebuah perangkat lunak yang dapat melakukan *Monitoring traffic* jaringan sekaligus *sniffing* , Namun tidak berlaku untuk semua *website* di karenakan beberpa website sudah terenripsi dengan baik.

#### 4.2 Saran

Dari penelitian ini penulis menyarankan beberapa hal yang berkaitan dengan software monitoring, dan sniffing di antaranya:

1. Meskipun wireshark dapat melakukan sniffing, alangkah baiknya jika di gunakan untuk kepentingan yang baik atau positif seperti dengan mengetahui

kekurangan dari suatu keamanan tertentu dapat lebih di tingkatkan lagi keamanan jaringannya.

2. Untuk menghindari sniffing dapat menggunakan keamanan firewall yang dapat menutup traffic yang datang baik incoming network traffic maupun outgoing network traffic berdasarkan sumber atau tujuan traffic tersebut.
3. Selain itu dapat menggunakan protocol yang memiliki standar aman yang sudah dilengkapi dengan enkripsi data seperti IPSec, HTTPS, SMB Signing, dan sebagainya.

### Daftar Pustaka

(Hanipah & Dhika, 2020) Analisa pencegahan aktivitas ilegal didalam jaringan dengan wireshark. *DoubleClick: Journal of Computer and Information Technology*, 4(1), 11-23.

(Hasbi & Saputra, 2022) Analisis Quality of Service (Qos) Jaringan Internet Kantor Pusat King Bukopin Dengan Menggunakan Wireshark. *JUST IT: Jurnal Sistem Informasi, Teknologi Informasi dan Komputer*, 12(1).

(Febriani & Sahfitri, 2022) MONITORING PENCEGAHAN AKTIVITAS ILEGAL DALAM JARINGAN PADA KANTOR DINAS ESDM PROVINSI SUMATERA SELATAN. In *Prosiding Seminar Hasil Penelitian Vokasi (Semhavok)* (Vol. 4, No. 1, pp. 92-99).

(Ubaedila et al., 2022) Layanan Jaringan Menggunakan Metode Sniffing Berbasis Wireshark. *INFORMATICS FOR EDUCATORS AND PROFESSIONAL: Journal of Informatics*, 6(1), 95-104.

(Wulandari & Ariyadi, 2022) ANALISA MONITORING SNIFFING PAKET DATA JARINGAN LOKAL PADA DINAS KOMUNIKASI DAN INFORMATIKA KOTA PRABUMULIH. In *Prosiding Seminar Hasil Penelitian Vokasi (Semhavok)* (Vol. 3, No. 2, pp. 185-192).

(Sulicdio et al., 2022) Comparative Analysis of Wireshark and Windump Software in Network Security Monitoring. *Jurnal Media Computer Science*, 1(1), 1-6.

(ALKASAR & Stiawan, 2020). *SISTEM PENCEGAHAN SERANGAN SQL INJECTION PADA WEB PENETRATION TESTING DAMN VULNERABLE WEB ATTACK DVWA MENGGUNAKAN METODE BAYESIAN NETWORK* (Doctoral dissertation, Sriwijaya University).

(Herman et al., 2023) Analisis Keamanan Jaringan LAN Terhadap Kerentanan Jaringan Ancaman DDoS Menggunakan Metode Penetration. *JURIKOM (Jurnal Riset Komputer)*, 10(1), 317-329.

(Setiawan & Zulfikri, 2020) Sistem Keamanan Jaringan Komputer Metode Network Intrusion Detection System Di Kantor Setwan. *Jurnal Intra Tech*, 4(2), 35-46.

(Ibrahim, 2020)). *Analisis Keamanan Jaringan pada Fasilitas Internet (Wifi) Kantor Pemerintahan Kota Batam terhadap Serangan Packet Sniffing* (Doctoral dissertation, Prodi Teknik Infomatika).

(Tamsir Ariyadi & Ali, 2018). Analisis Paket DHCP Rogue Pada Jaringan Local Area Network (LAN) Menggunakan Wireshark. In *PROSIDING SEMINAR NASIONAL INOVASI, TEKNOLOGI DAN APLIKASI SeNITiA-2018* (pp. 97-101). FAKULTAS TEKNIK UNIVESITAS BENGKULU

# ANALISA MONITORING UNTUK PENCEGAHAN AKSES ILEGAL DI DALAM JARINGAN DEPARTEMEN TI PT.PUSRI

*MONITORING ANALYSIS FOR THE PREVENTION OF ILLEGAL ACCESS WITHIN  
THE NETWORK OF THE IT DEPARTMENT OF PT. PUSRI*

M.Alzi Ikrar Agamuri<sup>1</sup>, Tamsir Ariyadi M.Kom<sup>2</sup>,  
<sup>1,2,3</sup>Universitas Bina Darma Palembang  
E-mail: <sup>1</sup>Alziikrar@gmail.com, <sup>2</sup>penulis.2@email.ac.id,

## Abstrak

Teknologi memegang peranan penting kelangsungan hidup manusia dalam aktivitas sehari-hari tidak lepas dari teknologi. Teknologi informasi memudahkan manusia berbagi informasi atau mencari informasi. Serangan siber seperti serangan *malware* atau upaya peretasan merupakan ancaman serius bagi jaringan TI. Tujuan dari keamanan jaringan adalah untuk mengantisipasi resiko ancaman jaringan yang dapat mengganggu operasional jaringan komputer sehari-hari. Dalam penelitian kali ini penulis menggunakan metode *Action Research*. Davison, ini di bertujuan untuk pengujian dan pengembangan, menemukan dan merancang. Jaringan pada Departemen TI PT. Pupuk Srwidjaja Palembang sudah cukup aman di karenakan pada saat di lakukannya monitoring jaringan selama 10 hari pada tanggal 6 juni 2023 sampai dengan 22 juni 2023 tidak ada terjadinya akses ilegal.

Kata Kunci : Wireshark, Monitoring, Teknologi, PT.Pusri

## Abstract

*Technology plays an important role in human survival in daily activities cannot be separated from technology. Information technology makes it easy for humans to share information or find information. Cyberattacks such as malware attacks or hacking attempts pose a serious threat to IT networks. The purpose of network security is to anticipate the risk of network threats that can disrupt daily computer network operations. In this study, the author used the Action Research method. Davison, this in aimed at testing and development, invented and designed. Network at the IT Department of PT. Pupuk Srwidjaja Palembang is quite safe because at the time of network monitoring for 10 days from June 6, 2023 to June 22, 2023 there was no illegal access..*

Keywords : Wireshark, Monitoring, Technology, PT. Pusri

## 1. PENDAHULUAN

Di era digitalisasi saat ini, teknologi memegang peranan penting kelangsungan hidup manusia dalam aktivitas sehari-hari tidak lepas dari teknologi. masalah ini berubah dari cara berpikir menjadi acuan bagi kemajuan peradaban manusia dan menangani dan memecahkan setiap masalah pola pikir yang kompleks agar tidak tersesat dengan perkembangan dan dukungan teknologi informasi didukung oleh berbagai penemuan dan inovasi banyak perubahan dalam hidup seseorang. Itu juga menyebabkan pengembangan bersama pembangunan dan teknologi Perangkat keras, secara langsung atau tidak langsung Informasi telah menjadi bagian penting dalam berbagai aspek kehidupan untuk dukungan sederhana tenaga kerja manusia. Departemen TI seringkali bertanggung jawab untuk mengelola dan menjaga keamanan data sensitif seperti informasi karyawan, informasi pelanggan, atau data bisnis penting lainnya. Monitoring dan

pengegasan akses ilegal membantu mencegah upaya pencurian atau pengungkapan data yang tidak sah di PT Pupuk Sriwidjaja (PUSRI).

Teknologi informasi memudahkan manusia berbagi informasi atau mencari informasi. kamu bisa melihatnya Tentang perkembangan teknologi internet dan jaringan. Baru-baru ini *internet* adalah untuk pertukaran informasi dan untuk mencari informasi. Jaringan komputer adalah suatu sistem yang terdiri dari beberapa komputer yang dirancang untuk pertukaran data, informasi dan sumber daya. Jaringan komputer adalah suatu sistem yang terdiri dari beberapa komputer yang dirancang untuk pertukaran data, informasi dan sumber daya. Tujuan dari jaringan komputer adalah Setiap bagian dari jaringan komputer dapat meminta dan menyediakan layanan informasi dan data. Pihak yang meminta atau menerima layanan kepada siapa pelanggan merujuk dan siapa yang mengirim atau menyampaikan layanan disebut *server*.

Serangan siber seperti serangan *malware* atau upaya peretasan merupakan ancaman serius bagi jaringan TI. Dengan memantau lalu lintas jaringan dan menerapkan tindakan pencegahan yang tepat, departemen TI dapat mengidentifikasi serangan yang sedang berlangsung dan mengambil tindakan untuk menghentikannya sebelum menjadi sangat merusak bagi perusahaan. Pada pasal 30 ayat 1 UU ITE No 19 Tahun 2016 ,Perbuatan ini dapat dikategorikan yang dinyatakan dalam Pasal 30 ayat (1) UU ITE yaitu setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun.

Tujuan dari keamanan jaringan adalah untuk mengantisipasi resiko ancaman jaringan yang dapat mengganggu operasional jaringan komputer sehari-hari. Nirkabel diperlukan di kantor karena nirkabel dapat membantu menyelesaikan pekerjaan. Perkembangan teknologi *Wireless Fidelity (WI-FI)* mengalami kemajuan yang sangat pesat untuk memenuhi kebutuhan sistem. Teknologi *WI-FI* banyak digunakan pada *hotspot* komersial, keamanan jaringan Internet *Service Provider (ISP)* di sekolah dan perkantoran sangat penting, namun hanya sebagian operator jaringan saja yang memperhatikan keamanan lalu lintas data pada jaringan *WI-FI*. Salah satu ancaman keamanan jaringan paling umum yang ditimbulkan oleh penjahat dunia maya adalah serangan paket. *Sniffing* paket adalah bentuk serangan yang menangkap data dari paket yang melintasi jaringan. Informasi ini mungkin termasuk nama pengguna, kata sandi, dan informasi penting lainnya yang dikirimkan melalui jaringan dalam bentuk teks. Tidak hanya satu paket yang harus ditangkap, bisa ratusan bahkan ribuan. Hal ini dapat merugikan pengguna jaringan komputer. Sero, R. L. (2022).

Dalam lingkungan TI yang kompleks, penggunaan ilegal atau aktivitas jaringan yang mencurigakan dapat mengganggu ketersediaan sistem. Dengan menggunakan solusi pemantauan yang tepat, departemen TI dapat mengidentifikasi masalah dan kesalahan jaringan dengan lebih cepat dan mengambil tindakan segera untuk menjaga ketersediaan sistem, Serangan yang berhasil dapat mengakibatkan gangguan pada proses bisnis. Mengontrol dan mencegah penggunaan ilegal dapat meminimalkan risiko kerusakan finansial dan reputasi yang mungkin diakibatkan oleh serangan atau pelanggaran keamanan.

Dalam penelitian ini penulis melakukan penelitian dengan menggunakan metode Action Research yang bertujuan untuk mengembangkan keterampilan-keterampilan baru atau cara-cara pendekatan baru dan untuk memecahkan masalah dengan cara penerapan langsung pada objek penelitian. Febriani, Y., & Sahfitri, V. (2022, August).

Sehubungan dengan hal tersebut di atas PT. Pupuk Sriwidjaja Palembang di perlukannya melakukan *monitoring* dan pencegahan dari akses ilegal pada jaringan menggunakan *wireshark*. *Administrator* jaringan dapat mengambil tindakan penanggulangan ketika akses ilegal terdeteksi melalui jaringan komputer akses ilegal yang di maksud adalah seperti pengguna atau user membuka situs atau webstie yang berbahaya dan tingkat keamanannya sangat lemah, Oleh karena itu *administrator* memerlukan alat yang tepat untuk memantau jaringan yaitu *wireshark*, *Software Wireshark* karena alat ini mampu menangkap paket data atau informasi dan sekaligus memantau lalu lintas antara Wlan (*Wireless Local area Network*). Febriani, Y., & Sahfitri, V. (2022, August).



## 2. METODE PENELITIAN

### 2.1 *Monitoring*

Monitoring merupakan aktivitas mengumpulkan dan menganalisis data berdasarkan faktor yang ditetapkan secara teratur kemudian berlanjut pada aktivitas program sehingga bisa melakukan tindakan koreksi untuk menyempurnakan aktivitas program tersebut

### 2.2 *Analisis*

Analisis adalah kegiatan untuk mencari pola, atau cara berpikir yang berkaitan dengan pengujian secara sistematis terhadap sesuatu untuk menentukan bagian, hubungan antar bagian, serta hubungannya dengan keseluruhan.

### 2.3 *Pengertian mencegah*

Menurut Kamus Besar Bahasa Indonesia (KBBI), kata mencegah /me•cegah/ dapat didefinisikan sebagai berikut.

- 1) Mengikhtiarkan supaya jangan terjadi
- 2) Merintang; melarang
- 3) Menahan agar sesuatu tidak terjadi; menegahkan; tidak menurutkan

### 2.4 *Wireless*

Wireless atau yang dikenal dengan jaringan nirkabel wireless atau wireless Network merupakan sekumpulan komputer yang saling terhubung antara satu dengan lainnya sehingga terbentuk sebuah jaringan komputer dengan menggunakan media udara/gelombang sebagai jalur lintas datanya. Teknologi wireless adalah salah satu pilihan yang tepat untuk menggantikan teknologi jaringan yang terdiri dari banyak kabel dan merupakan sebuah solusi akibat jarak antar jaringan yang tidak mungkin dihubungkan melalui kabel. Keuntungan terbesar dari wireless yaitu sangat praktis, dimana komputer dapat terhubung ke jaringan tanpa membutuhkan kabel.

### 2.5 *Web Traffic*

Traffic pada website merupakan jumlah orang yang mengunjungi website, membuka halaman website, dan durasi saat pengunjung membuka dan membaca halaman pada website kamu. Jadi, saat seseorang mengunjungi website kamu, kunjungan serta semua link yang mereka klik dan follow akan direkam oleh domain kamu. Nantinya angka-angka akan memberi ide tentang seberapa populernya website kamu.

### 2.6 *Cyber Crime*

Cyber Crime merupakan aktivitas individu maupun kelompok yang mengguakan jaringan komputer sebagai media untuk melakukan tindakan kriminal, atau menjadikan komputer sebagai sasaran kejahatan

### 2.7 *Jaringan Komputer*

Jaringan Komputer merupakan hubungan dengan beberapa perangkat yang bisa saling berkomunikasi satu sama lain. Perangkat yang dimaksud pada definisi ini mencakup komputer desktop, samrthphone, tablet, router, switch, dan hub

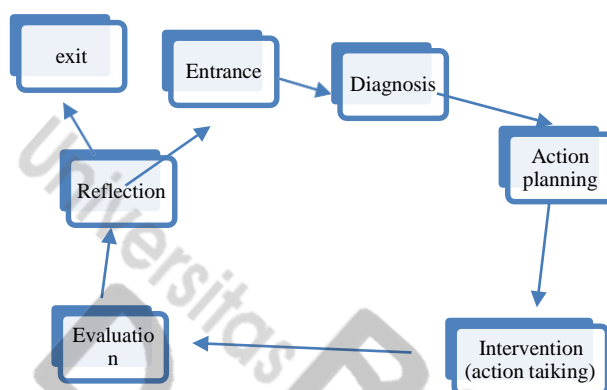
### 2.8 *Keamanan Jaringan*

Keamanan jaringan yang terkendalnya atas akses penggunaan jaringannya dimana seseorang dapat mengakses jaringan dan dikendalikan oleh siapapun yang berhak juga bisa menghalangi subjek maupun orang asing yang tidak memiliki hak untuk masuk ke dalam jaringan.

### 2.9 *Wireshark*

Wireshark merupakan tool yang ditunjukkan untuk menganalisa paket data jaringan, Wireshark juga disebut Network Packet Analyzer yang memiliki fungsi untuk menangkap paket data dalam jaringan dan berusaha memperlihatkan informasi dipaket tersebut secara rinci.

### 2.10 Dalam penelitian kali ini penulis menggunakan metode Action Research



Gambar 1. Metode Action Research

Davison, et al (2004) Metode *Reaction Research* ini di bertujuan untuk pengujian dan pengembangan, menemukan dan merancang, langkah-langkah ini diterapkan di tempat kerja (Objek), Dengan menggunakan metode ini pekerjaan akan menjadi lebih muda, lebih cepat dan hasilnya lebih baik dan lenih berkualitas.

### 2.11 Diagnose (Diagnosis)

Setelah melaksanakan magang di PT Pupuk Sriwidjaja Palembang, Peneliti Melakukan diagnosis setelah melihat beberapa karyawan mencoba masuk ke situs *web* yang mungkin belum memiliki standar keamanan, sehingga informasi pribadi seperti *Pasword* atau *email* dapat di kenali, Jika informasi penting seperti alamat email pengguna internet dapat di dideteksi meskipun email tersebut di tautkan ke banyak akun lain, ini dapat lebih berbahaya bagi pengguna unternet dan memungkinkan orang lain untuk menyalahgunakan.

### 2.12 Alat Alat yang Digunakan Topologi Pada PT. Pupuk Srwiridjaja

#### a. Router

Router merupakan salah satu komponen pada jaringan komputer yang mampu melewati data melalui sebuah jaringan atau internet menuju sasaran, melalui sebuah proses yang di kenal sebagai routing, Router berfungsi sebagai penghubung antar 2 (dua) atau lebih jaringan untuk meneruskan daa dari satu jaringan ke jaringan lainnya (Mhd. Dicky Syahpura LUBIS, dkk, 2020).

#### b. Proxy

Proxy adalah sistem yang menengahi pengguna dan internet untuk menyembunyikan identitas asli pengguna, sehingga data yang dikirim ke website tujuan akan menggunakan alamat IP dari proxy server, bukan alamat IP pengguna. (HeruKurniawan, dkk, 2020).

#### c. Hub

Hub adalah perangkat jaringan yang memungkinkan Anda menghubungkan beberapa PC ke satu jaringan. Perangkat ini digunakan untuk menghubungkan segmen

LAN. Sebuah hub memiliki berbagai macam port, jadi ketika sebuah paket tiba di satu port, itu disalin ke berbagai port lainnya. (Rizky Amanda, dkk, 2020).

d. Switch

switch adalah sebuah komponen jaringan yang tugasnya untuk menghubungkan beberapa perangkat, untuk bisa melakukan pertukaran paket data, baik dalam proses penerimaan, serta meneruskan data ke perangkat lain.(Desmira, dkk, 2020).

e. Kabel UTP

UTP merupakan singkatan dari Unshield Twisted Pair. Sesuai namanya "Unshield", yang berarti kabel ini tidak dilengkapi dengan pelindung aluminium sehingga jenis kabel ini kurang tahan dengan interferensi elektromagnetik, berbeda dengan saudaranya STP (Shield Twisted Pair).(Bobi Agustian, Muhammad Yasser Arafat,2020).

f. Kabel Fiber Optic

Fiber Optik adalah saluran transmisi atau sejenis kabel yang terbuat dari kaca atau plastik yang sangat halus dan lebih kecil dari sehelai rambut, dan dapat digunakan untuk mentransmisikan sinyal cahaya dari suatu tempat ke tempat lain. Sumber cahaya yang digunakan biasanya adalah laser atau LED.(Amalia Rizqi Utami, dkk, 2020).

g. Kabel Koaksial

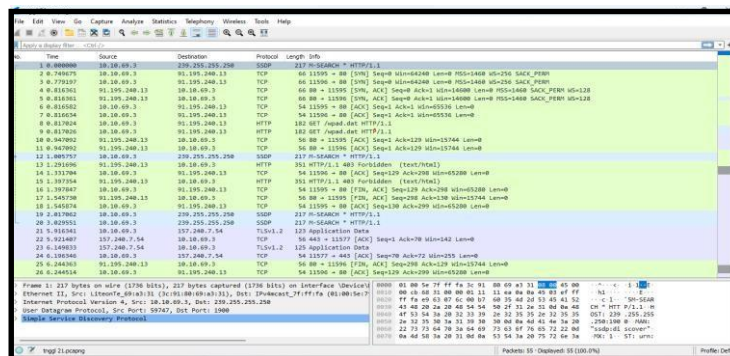
Kabel coaxial merupakan kabel yang mempunyai 2 konduktor yakni copper pada bagian tengahnya atau pusat inti yang terbuat dari tembaga bertekstur keras dan dilapisi dengan isolator. Sementara konduktor kedua adalah yang melingkar pada bagian luar isolator pertama serta tertutup dengan insulator luar.(Anisa Yulia Haryanti, dkk, 2021)

### 3. HASIL DAN PEMBAHASAN

#### 3.1 Filtering Protokol HTTP

Disini penulis akan mmelakukan filtering paket data yang melewati protokol http pada beberapa jaringan yang ada di PT.Pupuk Sriwidjaja Palembang, selanjutnya ketikkan http pada kolom address filter.

#### 1. capturing filtering pada jaringan pusri.id new



Gambar 2.filtering protocol http

Bisa di analisis user-agent yang di pakai pada jaringan Pusri.id New menggunakan Mozilla/5.0 (windows NT 10.0; WIN 64; x64) AppleWebKit/537.36 (KHTML, Like gecko) Chrome/115.0.0.0 Safari /537/36 Dan Host mysql - phi – intergration.com, Selain itu dapat di ketahui date yaitu 22 juni 2023 01:32 41 GMT DAN Full Request Get Uri Http, Disini bisa di

lihat bahwa adanya aktivitas yang sedang mengakses laman web Gambar Capture TCP Stream Wireshark dibawah ini dapat melihat info get yang sedang di buka



Gambar 3. *Tcp Stream*

Tabel 1. Website yang di akses pengguna pada jaringan PT.Pusri

NO	Website Yang Di Akses	Jenis Brwoser
1	http://mysql-phi-integration	Google Mozila
2	Blog.spot.com	Google Mozila
3	<a href="http://www.msftconnecttest.com">www.msftconnecttest.com</a> ,	Google Mozila
4	ocsp,pki.goog	Google Mozila

Tabel 2. data ip akses *protocol http*

TIME	SOURCE	DESTNATION	PROTO COL
0.069188	10.10.69.3	91.195.240.13	HTTP
650.037090	103.121.18.202	192.168.11.17	HTTP
86.281421	10.10.70.97	142.251.12.94	HTTP
72.863219	10.10.69.3	204.79.197.203	HTTP

#### 4. KESIMPULAN DAN SARAN

##### 4.1 Kesimpulan

Adapun penelitian pada jaringan di Departement TI PT. Pupuk Sriwidjaja Palembang adalah sebagai berikut.

1. Jaringan pada Departement TI PT. Pupuk Srwidjaja Palembang sudah cukup aman di karenakan pada saat di lakukannya monitoring jaringan selama 10 hari pada tanggal 6 juni 2023 sampai dengan 22 juni 2023 tidak ada terjadinya akses illegal.
2. Wireshark memiliki keunggulan pada bagian *sniffing* di bandingkan software monitoring lainnya dan wireshark juga dapat membaca hasil *capture* dari *software monitoring* lainnya.
3. Wireshark adalah sebuah perangkat lunak yang dapat melakukan *Monitoring traffic* jaringan sekaligus *sniffing* , Namun tidak berlaku untuk semua *website* di karenakan beberapa website sudah terenkripsi dengan baik.

Kesimpulan harus mengindikasi secara jelas hasil-hasil yang diperoleh, kelebihan dan kekurangannya, serta kemungkinan pengembangan selanjutnya. Kesimpulan dapat berupa paragraf, namun dapat juga berbentuk poin-poin dengan menggunakan numbering atau bullet. Saran-saran untuk untuk penelitian lebih lanjut untuk menutup kekurangan penelitian.

#### 4.2 Saran

Dari penelitian ini penulis menyarankan beberapa hal yang berkaitan dengan software monitoring, dan sniffing di antaranya:

1. Meskipun wireshark dapat melakukan sniffing, alangkah baiknya jika di gunakan untuk kepentingan yang baik atau positif seperti dengan mengetahui kekurangan dari suatu keamanan tertentu dapat lebih di tingkatkan lagi keamanan jaringannya.
2. Untuk menghindari sniffing dapat menggunakan keamanan firewall yang dapat menutup traffic yang datanf baik incoming network traffic maupun outgoing network traffic berdasarkan sumber atau tujuan traffic tersebut.
3. Selain itu dapat menggunakan protocol yang memiliki standar aman yang sudah di lengkapi dengan enkripsi data seperti IPSec, HTTPS, SMB Signing, dan sebagainya.

#### UCAPAN TERIMA KASIH

Terimakasih kepada PT.Pupuk Sriwidjaja Palembang dan Universitas Bina darma yang telah mendukung keterlaksanaannya penelitian ini

#### DAFTAR PUSTAKA


- [1] (Hanipah & Dhika, 2020) Analisa pencegahan aktivitas ilegal didalam jaringan dengan wireshark. *DoubleClick: Journal of Computer and Information Technology*, 4(1), 11-23.
- [2] (Hasbi & Saputra, 2022) Analisis Quality of Service (Qos) Jaringan Internet Kantor Pusat King Bukopin Dengan Menggunakan Wireshark. *JUST IT: Jurnal Sistem Informasi, Teknologi Informasi dan Komputer*, 12(1).
- [3] (Febriani & Sahfitri, 2022) MONITORING PENCEGAHAN AKTIVITAS ILEGAL DALAM JARINGAN PADA KANTOR DINAS ESDM PROVINSI SUMATERA SELATAN. In *Prosiding Seminar Hasil Penelitian Vokasi (Semhavok)* (Vol. 4, No. 1, pp. 92-99).
- [4] (Ubaedila et al., 2022) Layanan Jaringan Menggunakan Metode Sniffing Berbasis Wireshark. *INFORMATICS FOR EDUCATORS AND PROFESSIONAL: Journal of Informatics*, 6(1), 95-104.

- [5] (Wulandari & Ariyadi, 2022) ANALISA MONITORING SNIFFING PAKET DATA JARINGAN LOKAL PADA DINAS KOMUNIKASI DAN INFORMATIKA KOTA PRABUMULIH. In *Prosiding Seminar Hasil Penelitian Vokasi (Semhavok)* (Vol. 3, No. 2, pp. 185-192).
- [6] (Sulicdio et al., 2022) Comparative Analysis of Wireshark and Windump Software in Network Security Monitoring. *Jurnal Media Computer Science*, 1(1), 1-6.
- [7] (ALKASAR & Stiawan, 2020). *SISTEM PENCEGAHAN SERANGAN SQL INJECTION PADA WEB PENETRATION TESTING DAMN VULNERABLE WEB ATTACK DVWA MENGGUNAKAN METODE BAYESIAN NETWORK* (Doctoral dissertation, Sriwijaya University).
- [8] (Herman et al., 2023) Analisis Keamanan Jaringan LAN Terhadap Kerentanan Jaringan Ancaman DDoS Menggunakan Metode Penetration. *JURIKOM (Jurnal Riset Komputer)*, 10(1), 317-329.
- [9] (Setiawan & Zulfikri, 2020) Sistem Keamanan Jaringan Komputer Metode Network Intrusion Detection System Di Kantor Setwan. *Jurnal Intra Tech*, 4(2), 35-46.
- [10] (Ibrahim, 2020)). *Analisis Keamanan Jaringan pada Fasilitas Internet (Wifi) Kantor Pemerintahan Kota Batam terhadap Serangan Packet Sniffing* (Doctoral dissertation, Prodi Teknik Infomatika).
- [11] (Tamsir Ariyadi & Ali, 2018). Analisis Paket DHCP Rogue Pada Jaringan Local Area Network (LAN) Menggunakan Wireshark. In *PROSIDING SEMINAR NASIONAL INOVASI, TEKNOLOGI DAN APLIKASI SeNITiA- 2018* (pp. 97-101). FAKULTAS TEKNIK UNIVESITAS BENGKULU

### LOGBOOK MAGANG

Nama : M. Alzi Iktar Agamuri  
NIM : 201220020  
Mitra/DUDI : PT. Pupuk Sriwidjaja Palembang  
Waktu Magang : 21 Maret - 21 Juni 2023

No	Hari/Tanggal	Uraian Kegiatan
1	21 Maret 2023	Memperiapkan perlengkapan magang
2	24 Maret 2023	Pengarahan dari Diebat PT. PUSRI
3	27 Maret 2023	Pengujian dan pengarahan dari Rumbung KP
4	28 Maret 2023	Melakukan Perancangan Project
5	29 Maret 2023	Perancangan website absensi karyawan yang akan di bangun
6	30 Maret 2023	Melakukan penginstalan Aplikasi yang akan di gunakan

Pendamping Lapangan,  
  
(Achmad Fadhilansyah)




## LOGBOOK MAGANG

Nama : M. Alzi Ikrar Agamuri  
NIM : 201220020  
Mitra/DUDI : PT. PUPUK SRIWIDJAJA Palembang  
Waktu Magang : 21 Maret - 21 Juni 2023

No	Hari/Tanggal	Uraian Kegiatan
7	31 Maret 2023	Melakukan pembuatan rancangan di aplikasi visual code
8	3 April 2023	Membuat rancangan fitur home
9	4 April 2023	Melakukan pengecekan Troubleshoot di area TI
10	5 April 2023	Perbaikan komputer di Departement 1
11	6 April 2023	Perbaikan pengkabelan di Departement 1
12	10 April 2023	Lanjut rancangan Data Absensi

Pendamping Lapangan,

  
(Achmad Fadhlansyah...)



### LOGBOOK MAGANG

Nama : M. ARI IKRAR AGAMURI  
 NIM : 201220020  
 Mitra/DUDI : PT. PUPUK SRIWIDJAYA Palembang  
 Waktu Magang : 21 Maret - 21 Juni 2023

No	Hari/Tanggal	Uraian Kegiatan
13	13 April 2023	Memperiapkan ruangan rapat untuk rapat seluruh mahasiswa magang
14	14 April 2023	Petancangan menu absensi karyawan
15	17 April 2023	Petancangan codingan website di Laravel
16	18 April 2023	Konsultasi pada pembimbing mengenai proyek
17	27 April 2023	Penginputan data karyawan pada visual code
18	208 April 2023	Melakukan pembersihan komputer pada Gedung T1

Pendamping Lapangan,




(Achmad Fachhlansyah)

LOGBOOK MAGANG

Nama : M. ALZI IKRAR - A  
 NIM : 201220020  
 Mitra/DUDI : PT. Pupuk Sriwidjaya  
 Waktu Magang : 21 Maret - 21 Juni

No	Hari/Tanggal	Uraian Kegiatan
19	2 Mei 2023	Melakukan Persiapan untuk Report
20	3 Mei 2023	Melakukan pengecekan komputer dan perbaikan komputer
21	4 Mei 2023	Bimbingan project
22	5 Mei 2023	Perancangan DESIGN menu project
23	8 Mei 2023	Perancangan fitur absensi masuk karyawan
24	9 Mei 2023	Perbaikan monitor di TI

Pendamping Lapangan,


  
 (. A. M. H. Fauzan Sidiq )

### LOGBOOK MAGANG

Nama : M. Alzi (KPAR. A)  
 NIM : 201220020  
 Mitra/DUDI : RT. PUPUK Sriwidjaya  
 Waktu Magang : 21 Maret - 21 Juni

No	Hari/Tanggal	Uraian Kegiatan
25	10 Mei 2023	Pengecekan komputer di Gedung +1
26	11 Mei 2023	Melakukan Perbaikan Printer dan kabelan
27	12 Mei 2023	Melanjutkan Project dan bimbingan KP
28	15 Mei 2023	Menambahkan beberapa logo pada menu home
29	16 Mei 2023	Melakukan kunjungan ke pabrik untuk Perbaikan kabelan
30	17 Mei 2023	Memindahkan berkas arsip

Pendamping Lapangan,


  
 (. Achmad Fadlansyah .....)

### LOGBOOK MAGANG

Nama : M. ALZI IKRAR AGAMURI  
NIM : 201220020  
Mitra/DUDI : PT. PUPUK SRIWIDJATA  
Waktu Magang : 21 Maret - 21 Juni

No	Hari/Tanggal	Uraian Kegiatan
31	22 mei 2023	Melakukan Pengecekan komputer karyawan
32	23 mei 2023	Menambahkan Data nama karyawan Pada Codingan visual code
33	24 mei 2023	Menambahkan Data absensi Realtime
34	25 mei 2023	Menambahkan Template sidik Jari
35	29 mei 2023	Menambahkan Bodge karyawan
36	30 mei 2023	Menambahkan lokasi unit kerja Pada Visual code

Pendamping Lapangan,


  
(Ahmad Fadliunggrah...)

### LOGBOOK MAGANG

Nama : ██████████ M. ALZI IKRAR. A  
 NIM : 201220020  
 Mitra/DUDI : PT. PUPUK Sriwidjaja Palembang  
 Waktu Magang : 21 Maret - 21 Juni

No	Hari/Tanggal	Uraian Kegiatan
37	31 Mei 2023	Memperbaiki CPU dan komputer.
38	5 Juni 2023	Melakukan Perbaikan monitor dan LAN
39	6 Juni 2023	Memulai menyusun Laporan Kersa Praktek
40	7 Juni 2023	Membantu Pemindahan komputer
41	8 Juni 2023	Mempersiapkan rapat Bulanan Karyawan
42	9 Juni 2023	memonitoring jaringan wifi yang ada di pusri

Pendamping Lapangan,

  
 (Achmad Fadlansyah)



### LOGBOOK MAGANG

Nama : M. Azli Ikrar .A  
 NIM : 201720020  
 Mitra/DUDI : PT. PUPUK Sriwidjara  
 Waktu Magang : 21 Maret - 21 Juni

No	Hari/Tanggal	Uraian Kegiatan
43	12 Juni 2023	Melakukan perbaikan komputer
44	13 Juni 2023	Melakukan kegiatan sosialisasi Pegawai Pustri
45	14 Juni 2023	Pemasangan LAN pada komputer
46	15 Juni 2023	Membuat Laporan Kerja Praktek
47	16 Juni 2023	Membuat daftar list jadwal kegiatan Pegawai
48	18 Juni 2023	Memonitoring jaringan wifi dari Pencegahan Akses Ilegal

Pendamping Lapangan,

*Achmad Fadliansyah*  
 (Achmad Fadliansyah)

### LOGBOOK MAGANG

Nama : M. ALFI IKRAR. A  
NIM : 2017200120  
Mitra/DUDI : PT. PUPUK SEWIDJAJA  
Waktu Magang : 21 maret - 21 Juni

No	Hari/Tanggal	Uraian Kegiatan
49	20 Juni 2023	Melakukan Perpisahan kepada Pembimbing dan karyawan Pusri.
50	21 Juni 2023	Mengumpulkan laporan KP ke diklat PUSRI.

Pendamping Lapangan,

*CP*

(Achmad Padliansyah)



# PUPUK SRIWIDJAJA PALEMBANG

## SURAT KETERANGAN

Nomor : 432 /TB200.KP/2023

Menerangkan bahwa yang tersebut di bawah ini :

NAMA : M. Alzi Ikrar Agamuri  
NIM : 201220020  
JURUSAN : TEKNIK KOMPUTER  
UNIVERSITAS BINA DARMA

Telah selesai melaksanakan **Kerja Praktik**  
tanggal 21 Maret 2023 - 21 Juni 2023  
Dengan nilai : 8,57

di

**Departemen Mitra Bisnis & Layanan TI**  
**PT Pupuk Sriwidjaja Palembang**

Palembang, 11 Juli 2023

**Departemen Pembelajaran & Pengembangan SDM**

  
**Nola Sangkuntala**  
Vice President

Kantor Pusat  
Jalan Mayor Zen,  
Palembang 30118 - Indonesia  
Telp. (0711) 712111 / 712222  
Faks. (0711) 712100

[www.pusri.co.id](http://www.pusri.co.id)  
PT Pupuk Sriwidjaja Palembang  
is a subsidiary of  
PT PUPUK INDONESIA (Persero)





## FORMULIR

### Permohonan Pengajuan Judul TA/Skripsi

Nomor Dok	:	FRM/PKL/01/01
Nomor Revisi	:	02
Tgl. Berlaku	:	01 Februari 2020
Klausula	:	7.5

Palembang, 13 April 2023

Perihal : Permohonan Judul & Pembimbing  
TA/SKRIPSI

Kepada Yth.  
Ketua Program Studi Teknik Komputer  
Fakultas Vokasi  
Universitas Bina Darma  
Di -  
Palembang

Dengan hormat,  
Saya yang bertanda tangan dibawah ini, Mahasiswa Program Studi Teknik Komputer Universitas Bina Darma Palembang.

Nama : M.Alzi Ikrar Agamuri  
Nim : 201220020  
Semester : 6 (Enam)  
Program Studi : Teknik Komputer

Dengan ini mengajukan judul dan pembimbing Tugas Akhir / Skripsi, adapun judul yang saya ajukan sebagai berikut.

1. Analisa Monitoring untuk Pencegahan Akses Ilegal di dalam Jaringan Departemen TI RT PUPUC Sriwidjaja Palembang.
- Atas perhatiannya, saya ucapkan terima kasih.

Ketua Program Studi,

(Timur Dali Purwanto, M.Kom)

Hormat saya,

(M.Alzi Ikrar Agamuri)

Pembimbing TA/Skripsi : Tamsir Ariyadi M.KOM

  
30/5/2023

#### Syarat Pengajuan Judul

- Formulir di isi lengkap
- Photocopy KRS yang tercantum PKL
- Fotocopy lembar PA yang sudah diacc oleh Pembimbing Akademik untuk mengajukan PKL (Khusus Program Studi Sistem Informasi)
- Berkas dimasukkan dalam Map Plastik Transparan warna (Fak. Ilmu Komputer = Merah), (Fak. Ekonomi dan Bisnis = Kuning), (Fak. Bahasa & Sastra, Fak. Psikologi, dan Fak. Komunikasi = Biru) (Fak. Teknik = Hijau), (Fak. Ilmu Keguruan dan Ilmu Pendidikan = Merah Maroon), (Fak. Vokasi = Orange muda).

KEPUTUSAN  
DEKAN FAKULTAS VOKASI  
NOMOR : 009/SK/FV-TK/Univ-BD/VIII/2023  
TENTANG

PEMBIMBING PENELITIAN MAHASISWA  
FAKULTAS VOKASI UNIVERSITAS BINA DARMA

- Menimbang :
- Bahwa mahasiswa semester akhir diharuskan melaksanakan penelitian dan menyusun skripsi sebagai salah satu syarat untuk menyelesaikan studi pada Program Diploma 3 (D-3) Fakultas Vokasi Universitas Bina Darma;
  - Bahwa untuk kelancaran dalam pelaksanaan penelitian dan penyusunan skripsi dimaksud, dipandang perlu untuk menunjuk dan menugaskan Pembimbing Skripsi bagi setiap mahasiswa;
  - Bahwa untuk memenuhi butir-butir di atas perlu diterbitkan Surat Keputusan sebagai landasan hukumnya.
- Mengingat :
- Undang-undang Nomor 20 tahun 2003;
  - Peraturan Pemerintah Nomor 60 tahun 1999;
  - Akte Pendirian Yayasan Nomor 95 tanggal 28 Desember 1993;
  - Surat Keputusan Menteri Pendidikan Nasional Republik Indonesia Nomor : 112/D/O/2002;
  - Statuta Universitas Bina Darma;
  - Surat Keputusan Rektor Universitas Bina Darma Nomor : 165/SK/UNIV-BD/XI/2008 tanggal 03 Nopember 2008.

MEMUTUSKAN

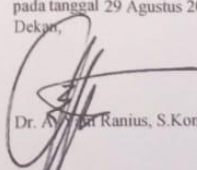
- Menetapkan :  
PERTAMA : Menunjuk dan menugaskan saudara-saudara
- Tamsir Ariyadi, M.Kom.
  -

berturut-turut sebagai Pembimbing Utama dan Pembimbing Pendamping dalam menyusun Skripsi mahasiswa di bawah ini :

Nama : M. Alzi Ikrar Agamuri  
Nim : 201220020  
Fakultas : Vokasi  
Program Studi : Teknik Komputer  
Judul Penelitian : ANALISA MONITORING UNTUK PENCEGAHAN AKSES ILEGAL DI DALAM JARINGAN DEPARTEMEN TI PT.PUPUK SRIWIDJAJA PALEMBANG

- KEDUA : keputusan ini berlaku mulai tanggal ditetapkan sampai dengan yang bersangkutan menyelesaikan skripsi dan tugas akhir,
- KETIGA : keputusan ini diberikan kepada yang bersangkutan untuk dilaksanakan sebagaimana mestinya, apabila di kemudian hari terdapat kekeliruan dalam penetapan ini akan diperbaiki sebagaimana mestinya.

Ditetapkan di Palembang  
pada tanggal 29 Agustus 2023  
Dekan,


  
Dr. Nur Hafid Ranius, S.Kom., M.M.

Tembusan disampaikan kepada Yth.  
1. Pembimbing Utama dan Pendamping;  
2. Ketua Program Studi;  
3. Mahasiswa yang bersangkutan.

**LEMBAR KONSULTASI KARYA AKHIR**

Nama : M. Alzi Ikrar Agamuri  
 NIM : 201220020  
 Fakultas : Vokasi  
 Program Studi : Teknik Komputer  
 Judul : ANALISA MONITORING UNTUK PENCEGAHAN AKSES ILEGAL DI DALAM JARINGAN DEPARTEMEN TI PT PUPUK SRWIDJAJA  
 Pembimbing : Tamsir Aryadi, M.Kom

No.	Tanggal	Uraian Konsultasi	Paraf
1	5/6/2023	- Penarikan Judul	PA
2	9/6/2023	- Jumlah referensi	PA
3	11/7/2023	- Formasi Pendirian bab 1-11	PA
4	1/8 2023	- Topologi	PA
5	5/8 2023	- Bab III	PA
6	12/8 2023	- Penarikan bab IV	PA
7	15/8 2023	- referensi 1	PA
8	22/8 2023	- referensi 1	PA
9	29/8 2023	- Acc Ujian 1	PA

	<b>FORMULIR</b>	Nomor Dak :	FRM/TA/05/09
	<b>Berita Acara Ujian Tugas Akhir Fakultas Vokasi</b>	Nomor Revisi :	00
		Tgl. Berlaku :	1 April 2015
		Klause ISO :	7,5

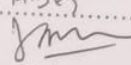


**Formulir**  
**Perbaikan Penulisan Tugas Akhir**  
*Program Studi Teknik Komputer, Komputerisasi Akuntansi,  
Manajemen Informatika, Manajemen Perusahaan,  
Administrasi Bisnis*  
**Fakultas Vokasi Universitas Bina Darma**

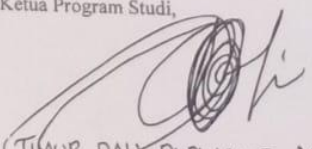
Nama Mahasiswa : M. ALZI IKRAR AGAMURI  
 Nim / Nirm : 201220020  
 Program Studi : TEKNIK KOMPUTER  
 Fakultas : VOKASI  
 Judul Tugas Akhir : ANALISA MONITORING UNTUK PENCEGAHAN AKSES ILEGAL DI DALAM JARINGAN DEPARTEMEN TI DT. PUPUK SRIWIDJAJA PADEMBANG

Catatan Perbaikan :
 

1. PERBAIKAN ABSTRAK ✓
2. TOPOLOGY JARINGAN -
3. ANALISA BEBERADA WI-FI
4. DIJELASKAN BERDASARKAN AKSES

Nama Penguji :
 

1. TAMSIR ARIYADI M.Kom (  )
2. IRWANSYAH M.M., M.Kom (  )
3. MISNEM S.Kom., M.Si. (  )

Mengetahui,  
 Ketua Program Studi,  
  
 (TIKUR DAH PURWANTO, M.Kom)



**SURAT KETERANGAN LULUS  
UJIAN TUGAS AKHIR  
PROGRAM STUDI TEKNIK KOMPUTER  
FAKULTAS VOKASI  
UNIVERSITAS BINA DARMA**



Nomor Dok : FRM/WDS/01  
Tanggal 01 Mei 2006, Rev. 00

Nama Lengkap : M. Alzi Ikrar Agamuri

NIM/NIRM : 201220020

Judul : Analisa Monitoring Untuk Pencegahan Akses Ilegal Di Dalam Jaringan Departemen Ti Pt.pupuk Sriwidjaja Palembang

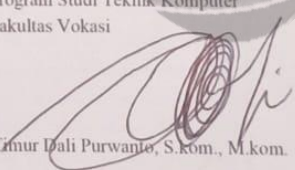
Pembimbing Utama : I. Tamsir Afiyadi, M.kom.

Telah mengikuti Ujian Akhir Program Studi Teknik Komputer Fakultas Vokasi Universitas Bina Darma pada

Hari/Tanggal : Sabtu, 09 September 2023

Dengan ini dinyatakan LULUS dengan score nilai 79 (B) dan dapat mengikuti Yudisium dan Wisuda. Atas perhatian dan kerjasamanya Kami mengucapkan terima kasih.

Palembang, 19 September 2023  
Program Studi Teknik Komputer  
Fakultas Vokasi

  
Timur Dali Purwanto, S.kom., M.kom.

**NB:**

1. Syarat untuk mendaftar Wisuda
2. Informasi Pendaftaran Wisuda Hubungi Pusat Pelayanan Mahasiswa
3. Wajib ditanda tangani oleh Ka.prog.Studi