ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

PROPOSAL TUGAS AKHIR

Disusun untuk Memenuhi Syarat Penulisan Tugas Akhir pada
Sekolah Tinggi Manajemen Informatika dan Komputer
(STMIK) Palangka Raya

OLEH:

LIANTONI
NIM C1957201023
PROGRAM STUDI SISTEM INFORMASI

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKA RAYA
2021

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

PROPOSAL TUGAS AKHIR

Disusun untuk Memenuhi Syarat Penulisan Tugas Akhir pada
Sekolah Tinggi Manajemen Informatika dan Komputer
(STMIK) Palangka Raya

OLEH:

LIANTONI
NIM C1957201023
PROGRAM STUDI SISTEM INFORMASI

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKA RAYA
2021

PERSETUJUAN

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Proposal Tugas Akhir Ini Telah Disetujui Untuk DiSeminarkan Pada
Tanggal 08 November 2021

Pembimbing I,

Sam'ani, ST., M.Kom.
NIK.197703252005105

Pembimbing II,

Hafiz Riyadli, M.Kom.
NIK. 198604042010103

Mengetahui :
Ketua STMIK Palangkaraya,

Suparno,M.Kom
NIK. 196901041995105

PENGESAHAN

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Proposal Tugas Akhir Ini Telah Diseminarkan, Dinilai dan Disahkan
Oleh Tim Penguji Seminar Pada Tanggal 08 November 2021

Tim Penguji Seminar Proposal :

1. Deden Andriawan, M.Kom.
   Ketua .....
2. Sam'ani, ST., M.Kom.
   Sekertaris .....
3. Norhayati, M.Pd.
   Anggota .....

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa yang telah memberikan suka cita serta kekuatan sehingga penulis dapat menyelesaikan Proposal Proposal Tugas Akhir ini dengan judul "Analisis Keamanan Jaringan Publik Pada Fasilitas Sosial Di Kota Palangka Raya Menggunakan Wireshark" terwujudnya proposal Proposal Tugas Akhir ini tidak lepas dari bantuan berbagai pihak yang telah mendorong dan membimbing penulis, baik tenaga, ide-ide, maupun pemikiran. Adapun tujuan penulisan Proposal Tugas Akhir ini adalah untuk memenuhi salah satu syarat penulisan Tugas Akhir pada Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya. Pada Kesempatan ini penulisan juga ingin menyampikan ucapan teriama kasih kepada.

1. Suparno,M.Kom selaku Ketua Sekolah Tinggi Manajmen Informatika dan komputer (STMIK) Palangkaraya;
2. Sam'ani, ST., M.Kom selaku dosen pembimbing I yang telah membimbing dalam materi topik penelitian secara keseluruhan.
3. Hafiz Riyadli, M.Kom selaku dosen pembimbing II yang telah membimbing dalam materi penulisan secara keseluruhan.
4. Deden Andriawan, M.Kom selaku dosen penguji seminar proposal Proposal Tugas Akhir.
5. Yang sangat istimewa orang tua dan keluarga penulis yang selalu

memberi dukungan semangat yang tidak henti-hentinya kepada penulis di dalam proses penulisan Proposal Tugas Akhir yang penulis tempun sekarang.

6. Seluruh teman-teman seperjuangan dan sepenanggung di Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya yang selalu memberikan dukungan semangat baik secara langsung maupun tidak langsung.

Penulis menyadari bahwa tak ada gading yang tak retak, begitu juga dengan Proposal Proposal Tugas Akhir ini yang tidak luput dari kekurangan.

Palangka Raya, November 2021

Penulis,

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

A. Latar Belakang

Seiring dengan perkembangan teknologi pada era sekarang internet merupakan hal yang sangat dibutuhkan oleh semua aspek kehidupan manusia, karena dengan internet kita bisa dengan mudah berkomunikasi dengan orang-orang yang berada jauh sampai keluar negeri melalui media sosial yang telah banyak disediakan sekarang, tidak hanya sebagai media komunikasi tetapi juga sebagai salah satu tempat mengekspresikan diri, dan internet juga dapat digunakan sebagai media untuk menyimpan data-data yang penting.

Untuk bisa terhubung ke dalam sebuah internet kita bisa menggunakan kabel ataupun wireless (*Wifi*), seperti yang kita ketahui seseorang bisa terkoneksi ke sebuah intenet kapanpun dan dimanapun selagi terdapat jaringan melalui media seperti komputer, laptop, tablet, *notebook*, ataupun smartphone.

Pada saat ini *issue* keamanan jaringan menjadi sangat penting dan patut untuk diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para hacker, baik jaringan *wired LAN* maupun wireless *LAN*. Pada saat data dikirimkan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak

bertanggung jawab untuk melakukan penyadapan atau mengubah data tersebut.

Dalam pembangunan perancangannya, sistem keamanan jaringan yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya Serangan ARP Spoofing merupakan serangan yang berbahaya karena dapat mendukung terjadinya serangan jaringan komputer lainnya seperti *Denial of Service, Man in the middle attack, host impersonating* dan lain-lain.

Dinas Komunikasi, Informatika Persandian dan Statistik Kota Palangka Raya telah menerapkan jaringan *wifi* gratis di beberapa fasilitas umum Kota Palangka Raya. Terdapat ada 5 jaringan yang terpasang pada tempat umum inilah yang sering rentan dari para hacker. Banyak pengguna jaringan *wifi* tidak bisa membayangkan jenis bahaya apa yang sedang menghampiri mereka pada saat sedang berasosiasi dengan *wireless access point* (*WPA*).

Berdasarkan latar belakang yang diuraikan diatas, maka peneliti tertarik untuk menganalisis suatu jaringan *wifi* yang ada pada fasilitas umum di Kota Palangka Raya dan mengangkat judul "**Analisis Keamanan Jaringan Publik Pada Fasilitas Sosial Di Kota Palangka Raya Menggunakan Wireshark***"*.

B. Rumusan Masalah

Pada penelitian ini terdapat rumusan permasalahan yang menjadi titik utama yaitu bagaimana cara mengalisis keamanan jaringan publik pada fasilitas sosial di kota palangka raya menggunakan *wireshark*.

C. Batasan Masalah

Adapun Batasan masalah dari penelitian ini supaya tidak terjadi kesalahan persepsi dan tidak meluaskan pokok bahasan yaitu.

1. Melakukan pengujian penetrasi pada *wifi* menggunakan tools *Wireshark* sehingga dapat menemukan celah yang tampak dari wifi tersebut
2. Penelitian ini tidak melakukan implementasi peningkatan keamanan jaringan yang sudah ada dan hanya memberikan cara yang tepat yang sebaiknya dilakukan untuk mengantisipasi dari terjadinya serangan *sniffing* (Pencurian Data) pada jaringan *Wifi.*
3. Adapun lokasi yang di analisis antara lain jaringan *wifi*.id non-berbayar pada taman Pasuk Kameloh Kota Palangka Raya.

D. Tujuan dan Manfaat

1. Tujuan

Tujuan dari pemilihan judul ini yaitu agar hasil dari penelitian yang dilakukan akan memberikan cara yang tepat untuk dapat mencegah terjadinya penyerangan *sniffing* saat mengakses jaringan

bebas atau terbuka pada fasilitas umum.

2. Manfaat

a. Manfaat bagi masyarakat STMIK Palangka Raya

Penelitian ini diharapkan dapat berguna bagi peneliti lainnya agar dapat di lanjutkan dan di kembangkan arah penelitian ini agar dapat lebih kritisi dalam menganalisis jaringan terbuka pada fasilitas umum lainnya

.

b. Manfaat bagi masyarakat luas

Penelitian ini di harapkan agar masyarakat luas dapat mengerti tentang keamanan jaringan yang ada pada fasilitas umum sehingga terhindar dari segala macam pencurian data pribadi pada *device* nya saat mengakses jaringan terbuka.

E. Jenis Penelitian

Dalam suatu penelitian seorang peneliti harus menggunakan jenis penelitian yang tepat. Hal ini dimaksud agar peneliti dapat memperoleh gambaran yang jelas mengenai masalah yang dihadapi serta langkah-langkah yang digunakan dalam mengatasi masalah tersebut.

Adapun jenis penelitian yang digunakan dalam penelitian ini adalah menggunakan metode penelitian Deskriptif kualitatif.

F. Sistematika Penulisan

Penulis memberikan gambaran terhadap pembahasan Laporan Proposal Tugas Akhir ini agar sesuai dengan tujuan, maka penulisan disusun dengan sistematika penulisan sebagai berikut,

BAB I PENDAHULUAN

Bab ini akan membahas mengenai latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat, sistematika penulisan, dan penjelasan istilah kunci.

BAB II LANDASAN TEORI

Bab ini menguraikan secara singkat mengenai dasar teori-teori yang berkaitan dengan judul laporan analisis ini dan Penelitian yang relevan.

BAB III METODE PENELITIAN

Dalam bab ini akan membahas tentang metode pengumpulan data, metode pengembangan sistem, tinjauan umum, analisis dan hasil penelitian.

BAB IV PENUTUP

Dalam bab ini memuat kesimpulan dan saran-saran penulis dari penulisan yang telah dibahas.

G. Penjelasan Istilah Kunci

1. Jaringan Publik adalah jaringan yang dibangun oleh pemerintah maupun penyedia jasa telekomunikasi kepada publik, baik yang berorientasi profit maupun non-profit, sehingga masyarakat luas dapat memanfaatkannya dalam bertukar informasi.
2. *Wifi* Kependekan Dari *Wireless Fidelity* Yaitu Sebuah Media Penghantar Komunikasi Data Tanpa Kabel Yang Bisa Digunakan Untuk Komunikasi Atau mentransfer Program Dan Data Dengan Kemampuan Yang Sangat Cepat.
3. *Wireshark* merupakan salah satu tools atau aplikasi capture paket data berbasis *open-source* untuk melakukan analisis dan pemecah masalah jaringan.
4. *Sniffing* adalah tindak kejahatan penyadapan yang dilakukan menggunakan jaringan internet dengan tujuan utama untuk mengambil data dan informasi sensitive secara illegal.
5. *Hacker* adalah istilah untuk seseorang yang mempelajari, memodifikasi, menganalisa dan masuk ke sebuah jaringan komputer.
6. *Wireless Access Point* adalah suatu sistem yang juga dapat diterapkan untuk mengamankan jaringan nirkabel.

BAB II

TINJAUAN PUSTAKA

A. Dasar Teori

1. yang berkaitan dengan topik penelitian

a. Analisis

Menurut Komaruddin (2001:53) Pengertian analisis adalah kegiatan berpikir untuk menguraikan suatu keseluruhan menjadi komponen sehingga dapat mengenal tanda-tanda komponen, hubungannya satu sama lain dan fungsi masing-masing dalam satu keseluruhan yang terpadu.

Menurut Harahap dalam (Azwar, 2019) Pengertian analisis adalah memecahkan atau menguraikan sesuatu unit menjadi unit terkecil. Dari pendapat diatas dapat ditarik kesimpulan bahwa analisis merupakan suatu kegiatan berfikir untuk menguraikan atau memecahkan suatu permaslaahan dari unit menjadi unit terkecil.

Menurut Yuni (2020) Pengertian analisis yang dikemukakan di atas, dapat disimpulkan bahwa analisis adalah bukan hanya sekedar penelusuran atau penyelelidikan, tetapi suatu kegiatan yang terencana dan dilakukan secara sungguh-sungggguh dengan menggunakan pemikiran yang kritis untuk memperoleh kesimpulan dari apa yang ditaksir.

Pengertian analisis yang dikemukakan di atas, dapat disimpulkan bahwa analisis adalah bukan hanya sekedar penelusuran atau penyelelidikan, tetapi suatu kegiatan yang terencana dan dilakukan secara sungguh-sungguh dengan menggunakan pemikiran yang kritis untuk memperoleh kesimpulan dari apa yang ditaksir.

b. Jaringan

Menurut Kustanto (2015:1) " Jaringan komputer adalah kumpulan dua atau lebih komputer yang saling berhubungan satu sama lain untuk melakukan komunikasi data dengan menggunakan protokol komunnikasi melalui media komunikasi (kabel atau nirkabel), sehingga komputer-komputer tersebut dapat saling berbagi informasi, data program-program, dan penggunaan perangkat keras secara bersama". Dalam hal ini komunikasi data yang bisa dilakukan melalui jaringan komputer dapat berupa data teks, gambar, vidio dan suara.

c. Keamanan Jaringan

Menurut Singh (2014), keamanan jaringan adalah melindungi informasi yang ada pada sistem informasi dari orang yang tidak memiliki hak akses atau hak untuk melakukan modifikasi terhadap informasi tersebut baik dari sisi penyimpanan, waktu proses ataupun saat informasi transit di suatu tempat. Keamanan

informasi adalah gabungan dari keamanan komputer dan juga keamanan komunikasi. Keamanan informasi bukan hanya keamanan komputer saja. keamanan informasi menyangkut lebih luas dibandingkan keamanan komputer, seperti memberikan keamanan pada informasi aset yang dimiliki dari pencurian ataupun bencana alam dan juga dari social attack engineering seperti seseorang melakukan penipuan kepada target agar dapat memberikan informasi yang sensitif kepadanya. Keamanan informasi adalah suatu proses untuk mengamankan informasi dari yang tidak berhak, menggunakan, merusak, memodifikasi, mendistribusikan informasi tersebut. Proses berulang ini melibatkan latihan terus menerus, penilaian, proteksi, memonitor, mendeteksi, merespon insiden dan memperbaiki, dan juga melakukan dokumentasi dan ulasan. Proses ini membuat keamanan informasi menjadi bagian yang tidak dapat dipisahkan dari segala operasi bisnis di semua kalangan.

d. Fasilitas Publik

Pengertian sarana dan prasarna Menurut Kamus Besar Bahasa Indonesia (KBBI) Sarana adalah segala sesuatu yang dapat dipakai sebagai alat dalam mencapai maksud atau tujuan. Sedangkan prasarana adalah segala sesuatu yang merupakan penunjang utama terselenggaranya suatu proses (usaha, pembangunan, proyek). untuk lebih memudahkan membedakan

keduanya. Sarana lebih ditujukan untuk benda-benda yang bergerak, sedangkan prasarana lebih ditujukan untuk benda-benda yang tidak bergerak seperti bangunan. Definisi fasilitas adalah segala sesuatu yang berbentuk benda maupun uang yang dapat memudahkan serta memperlancar pelaksanaan suatu usaha tertentu.

Menurut Sam (2008) Fasilitas umum adalah sarana yang disediakan untuk kepentingan umum seperti jalan raya, lampu penerangan jalan, halte, trotoar, dan jembatan penyebrangan. Fasilitas yang disediakan ini merupakan sarana yang memberikan kemudahan bagi masyarakat sehingga harus dipelihara dengan baik. Fasilitas pejalan kaki berfungsi memisahkan pejalan kaki dari jalur lalu lintas kendaraan guna menjamin keselamatan pejalan kaki dan kelancaran lalu lintas.

e. Wireshark

Wireshark merupakan salah satu tool aplikasi *Network Analyzer* atau analisa jaringan *open source*. Awalnya *tool* ini bernama *Ethereal*, pada Mei 2006 proyek ini berganti nama menjadi *Wireshark* karena masalah merek dagang. Penganalisaan kinerja jaringan itu dapat melingkupi berbagai hal, mulai dari proses menangkap pakrt-paket data atau informasi yang belalu-lalang dalam jaringan, sampai digunakan pula untuk *sniffing*, *sniffing* yaitu memperoleh informasi penting seperti *password*,

email, data sensitif, dan lain-lain. Tampilan *wireshark* ini sangat bersahabat karena mengguunakan tampilan grafis atau *GUI*.

Fungsi *Wireshark* antara lain berikut dibawah ini.

1) Menganalisa jaringan.
2) Menangkap paket data atau informasi yang berkeliaran dalam jaringan yang terlihat.
3) Penganalisaan informasi yang didapat dengan melakukan sniffing.
4) Membaca data secara langsung dari Ethernet, Token-Ring, FDDI, Serial (PPP dan SLIP), 802.11 wireless LAN, dan koneksi ATM.
5) Menganalisa transmisi paket data dalam jaringan, proses koneksi dan transmisi data antar komputer.

B. Penelitian Yang Relevan

Beberapa penelitian yang relevan dengan penelitian ini adalah.

1. Penelitian yang dilakukan oleh Agung Nugroho yang berjudul "Analisa Keamanan Jaringan Wireless Local Area Network Dengan Access Point Tp-Link Wa500g". Hasil penelitian ini menunjukkan bahwa pengujian terhadap keamanan pada jaringan wireless dari sisi keamanan access point, dan access point yang digunakan adalah TPLINK WA500G. Metode konsep yang digunakan adalah wireless hacking, pengujiannya

diantaranya meliputi reveal SSID (Service Set Identifier), MAC address spoofing , crack WEP (Wired Equivalent Privacy), crack WPA/WPA2 PSK (Wifi Protected Access Pre-Shared Key). Persamaan penelitian terdahulu dengan yang penulis teliti adalah terletak pada analisa jaringan wireless. Perbedaannya yaitu penelitian yang dilakukan sebelumnya untuk pengujian terhadap celah keamanan access point TP-LINK WA500G dapat memberikan pemahaman terhadap celah keamanannya dan cara untuk pencegahan wireless hacking sedangkan yang penulis teliti adalah untuk menganalisa keamanan jaringan publik untuk mengatasi kemungkinan masalah yang terjadi pada lalu lintas data menggunakan wireshark.

2. Penelitian yang dilakukan oleh M. R. Kurniawan yang berjudul "Analisis Sistem Keamanan Wireless Local Area Network (Wlan) Pada Proses Tethering". Hasil penelitian ini menunjukkan bahwa segi keamanan komunikasi data pada jaringan tersebut rentan terhadap aktivitas ilegal seperti sniffing dan scanning serta kejahatan lainnya. Persamaan penelitian terdahulu dengan yang penulis teliti adalah terletak pada analisa jaringan wireless. Perbedaannya yaitu penelitian yang dilakukan sebelumnya meneliti jaringan *tethering* sedangkan penulis meneliti jaringan *wifi* terbuka fasilitas sosial.
3. Penelitian yang dilakukan oleh Gilang Kumala Dewi yang

berjudul “Analisa Keamanan Jaringan *Wireless* Di Sekolah Menengah Al Firdaus”. Hasil penelitian ini menunjukkan bahwa celah pada keamanan yang diterapakan di jaringan wireless Sekolah Menengah Al Firdaus namun untuk saat ini keamanan yang diterapkan sudah tergolong cukup aman. Karena kebanyakan *access point* yang dipasang sudah menggunakan keamanan setingkat *WPA*/*WPA2*. Persamaan penelitian terdahulu dengan yang penulis teliti adalah terletak pada analisa jaringan *wireless*. Perbedaannya yaitu penelitian yang dilakukan sebelumnya meneliti jaringan sekolah sedangkan penulis meneliti jaringan *wifi* fasilitas sosial.

4. Penelitian yang dilakukan oleh Bayu Arie Nugroho yang berjudul “Analisis Keamanan Jaringan Pada Fasilitas Internet (*Wifi*) Terhadap Serangan *Packet Sniffing*”. Hasil penelitian ini menunjukkan bahwa Jaringan *wifi* sangat rentan terhadap ancaman serangan, karena komunikasi yang terjadi bersifat terbuka. Diperlukan *system* pengamanan yang baik untuk dapat menjaga keamanan data pengguna agar terhindar dari serangan yang dilakukan oleh orang–orang yang tidak bertanggung jawab. Penelitian ini membahas evaluasi tingkat keamanan fasilitas *wifi* di PT. Angkasa Pura I Bandar Udara Internasional Adi Sumarmo Surakarta dengan menggunakan aplikasi *netstumbler*, *inSSIDer* dan *ettercap*. Persamaan

penelitian terdahulu dengan yang penulis teliti adalah terletak pada analisa jaringan wireless. Perbedaannya yaitu penelitian yang dilakukan sebelumnya meneliti jaringan institusi BUMN sedangkan penulis meneliti jaringan terbuka fasilitas sosial.

5. Penelitian yang dilakukan oleh Ayu Syifa Destiani yang berjudul "Analisis Protokol Keamanan Situ Unpas Dengan Menggunakan *Sslstrip* Dan *Wireshark*". Hasil penelitian ini menunjukkan bahwa bahwa segi keamanan komunikasi data pada jaringan tersebut rentan terhadap aktivitas ilegal seperti *sniffing* dan *scanning* serta kejahatan lainnya akibat penggunaan aplikasi *NetCut* oleh pihak yang tidak bertanggung jawab. Persamaan penelitian terdahulu dengan yang penulis teliti adalah terletak pada analisa jaringan *wireless*. Perbedaannya yaitu penelitian yang dilakukan sebelumnya meneliti jaringan institusi BUMN sedangkan penulis meneliti jaringan terbuka fasilitas publik.
6. Penelitian yang di lakukan Oleh Aulia Rahmah (STMIK Palangka Raya) dengan judul Analisis Jaringan Wireless Pada Kampus STIE YBPK Palangka Raya, meneliti tentang jaringan serta *Qos (Quality of Service) WLAN* kampus STIE YBPK Palangka Raya. Persamaan dengan penulis ialah meneliti jaringan *Wireless*, sedangkan perbedaan dengan penulis ialah dari objek maupun *tools* yang digunakan.

7. Penelitian yang di lakukan Oleh Rizky Dwi M (STMIK Palangka Raya) dengan judul Analisis Sistem Monitoring Jaringan Pada SMPN 2 Pandih Batu Kabupaten Pulang Pisau Menggunakan *Wireshark*. Persamaan dengan penulis ialah sama menggunakan *tools Wireshark,* sedangakan perbedaanny adalah pada objek dan tipe jaringan yang diteliti oleh penulis.

BAB III

METODE PENELITIAN

A. Metode Penelitian

Metode yang digunakan adalah metode *Deskriptif kualitatif* yaitu menjelaskan tentang keadaan atau situasi yang terjadi. Tahap yang dilakukan adalah menggunakan kuisioner untuk mengukur level kematangan dari prosedur pengamanan yang sudah dilakukan. Kriteria penilaiannya di sesuaikan dengan kriteria penilaian CMM yang terdiri dari level 0 hingga level 5. Selanjutnya menggunakan form audit checklist untuk mengukur kondisi keamanan dari infrastuktur jaringan berupa mikrotik dan komputer. Kriteria penilaiannya adalah dengan menggunakan skala *guttman*, jawaban memiliki kriteria tegas yakni *yes* or *no*. selanjutnya akan dihitung persentase dari rata-rata setiap aspek yang dihitung berdasarkan hasil pengambilan data form audit dengan menggunakan rumus persentase

$$x = \frac{jk}{total} x\ 100\%$$

Dimana : x = Persentase pencapaian responden, jk = Jumlah keseluruhan skor yang di dapatkan dan total = Skor Maksimal

B. Metode Pengumpulan Data

Dalam penelitian, teknik pengumpulan data merupakan faktor penting demi keberhasilan penelitian. Hal ini berkaitan dengan

bagaimana cara mengumpulkan data, siapa sumbernya, dan apa alat yang digunakan.Jenis sumber data adalah mengenai dari mana data diperoleh. Apakah data diperoleh dari sumber langsung (data primer) atau data diperoleh dari sumber tidak langsung (data sekunder).

Metode Pengumpulan Data merupakan teknik atau cara yang dilakukan untuk mengumpulkan data. Metode menunjuk suatu cara sehingga dapat diperlihatkan penggunaannya melalui angket, wawancara, pengamatan, tes, dokumentasi dan sebagainya. Sedangkan Instrumen Pengumpul Data merupakan alat yang digunakan untuk mengumpulkan data. Karena berupa alat, maka instrumen dapat berupa lembar cek list, kuesioner (angket terbuka atau tertutup), pedoman wawancara, kamera foto dan lainnya. Adapun dua teknik pengumpulan data yang digunakan adalah pengamatan dan dokumentasi screenshoot. Berikut penjelasan dibawah ini.

1. Observasi

   Metode observasi adalah melihat dan mendengarkan peristiwa atau tindakan yang dilakuakan oleh orang-orang yang diamati, kemudian merekam hasil pengamatannya dengan catatan atau alat bantu lainnya.

2. Dokumentasi

   Studi dokumen adalah metode pengumpulan data yang tidak ditujukan langsung kepada subjek penelitian. Studi dokumen adalah

jenis pengumpulan data yang meneliti berbagai macam dokumen yang berguna untuk bahan analisis. Dokumen yang dapat digunakan dalam pengumpulan data dibedakan menjadi dua, yakni:

a. Dokumen primer

Dokumen primer yang penulis gunakan dalam penelitian ini yaitu Jurnal yang berhubungan dengan keamanan jaringan.

b. Dokumen sekunder

Dokumen sekunder yang penulis gunakan yaitu Buku pedoman jaringan komputer Telkom Indonesia.

C. Tinjauan Umum

Taman Pasuk Kameluh yang ada di bantaran Sungai Kahayan berdekatan dengan Tugu Soekarno, setiap hari selalu ramai dikunjungi warga yang ingin bersantai sambil menikmati suasana Sungai Kahayan. Taman Pasuk Kameluh, adalah salah satu tempat destinasi wisata yang ada di kota Palangka Raya. Tempat ini menjadi salah satu tempat iconik kota Palangka Raya. Taman Pasuk Kameluh diambil dari bahasa Dayak. Memiliki makna bakul gadis, yang artinya barang yang dimiliki seorang gadis. Kameloh lebih identik dekat dengan bakul perempuan cantik. Namun sebagian masyarakat juga mengartikan Pasuk Kameloh seperti kantong semar yang mengeluarkan panorama keindahan. Taman Pasuk

Kameluh menyediakan lahan parkir dan juga toilet umum. Tersedia juga masjid bagi pengunjung yang ingin melaksanakan ibadah. Di taman ini memancar wifi dan terdapat kamera CCTV. Di bawah jembatan Kahayan terhampar kawasan kuliner khas Kalimantan.

Pada taman pasuk kameluh terdapat jaringan bebas yang disedaikan kolaborasi Pemerintah Kota dan Telkom Indonesia yang mana diperuntukan bagi pengunjung taman tersebut.

D. Analisis

1. Analisis keamanan jaringan yang sedang berjalan

   Sistem keamanan jaringan pada saat ini masih kurang efektif dan efisien dalam mensimulasikan tingkat keamanan pada jaringan internet. Dimana keamanan jaringannya masih memiliki celah yang dapat disusupi pihak-pihak yang tidak bertanggung jawab.

   Maka dari itu penulis mengangkat judul ini agar dilaksanakannya penelitian terhadap keamanan jaringan terbuka pada taman pasuk kameluh menggunakan *tool wireshark*.

2. Analsis sistem yang diusulkan

   Analisis sistem yang diusulkan yaitu identifikasi celah keamanan jaringan pada website dengan tools packet sniffer untuk mengaudit keamanan jaringan dan memblokir lalu lintas jaringan yang dianggap sebagai ancaman dalam jaringan internet serta melakukan pengecekan terhadap kesalahan pada bagian media, wireless, dan media koneksinya.

3. Analisis Kebutuhan Analisis

Analisis kebutuhan analisis sangat diperlukan dalam mendukung analisis algoritma, apakah telah sesuai dengan kebutuhan atau belum. Karena kebutuhan analisis akan mendukung tercapainya tujuan.

a. Kebutuhan Perangkat Keras

Kebutuhan perangkat keras yang digunakan untuk menganalisis keamanan jaringan fasilitas sosial berikut dibawah ini.

1) Processor Intel Core i3 2.3GHz atau lebih

2) RAM minimal 2GB

3) Harddisk Minimal 8GB untuk instalasi software

4) Wifi Dongel Wireless

b. Kebutuhan Perangkat Lunak

Kebutuhan perangkat lunak yang digunakan untuk menganalisis keamanan jaringan fasilitas sosial berikut dibawah ini.

1) WireShark

2) NetCap

3) Google Chrome

c. Kebutuhan Informasi

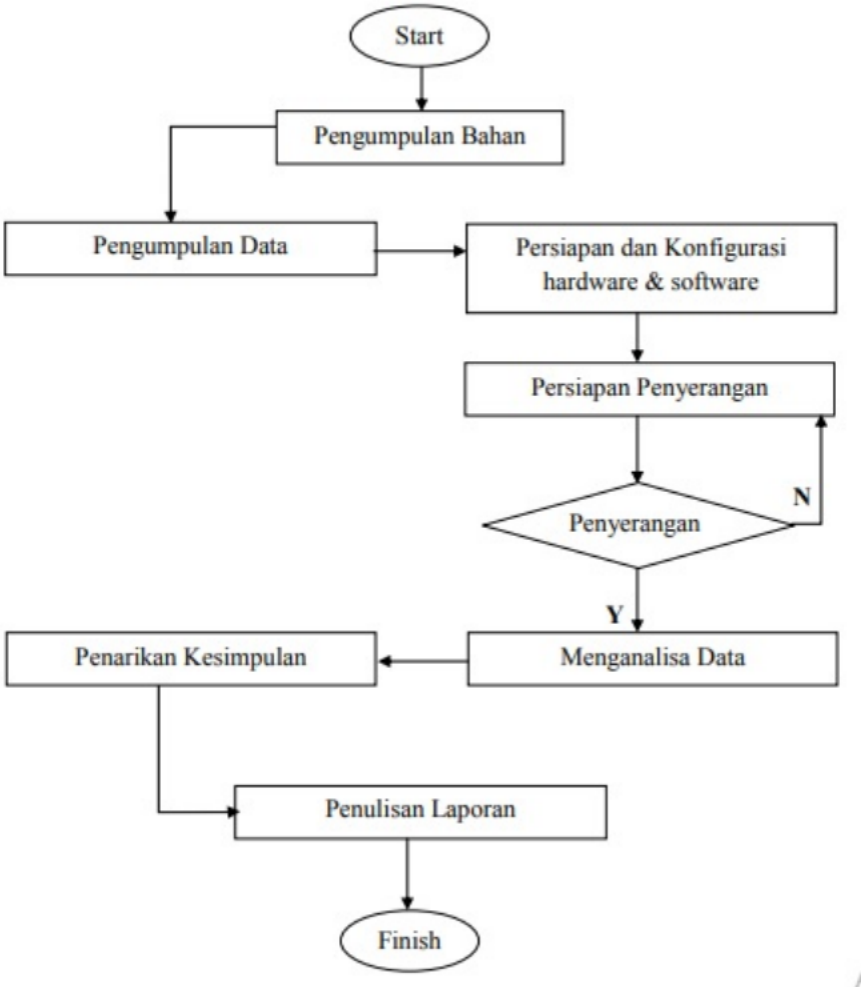
Kebutuhan informasi yang dibutuhkan penulis antara lain.

1) Literasi tentang Wireshark

2) Literasi tentang Jaringan Komputer

4. Kerangka Pemikiran dan flowchart

Dalam menjelaskan sebuah permasalahan kerangka pemikiran atau alur penelitian disajikan untuk mempermudah pemahaman dalam penelitian tersebut. Metode tersebut tersaji dalam diagram alir penelitian. Berikut dibawah ini.



Gambar 1. Flowchart Penelitian

5.Teknis Pengujian Keamanan

Pengujian keamanan bertujuan untuk memperoleh kesadaran akan

permasalahan keamanan pada jaringan kabel dan nirkabel (wireless LAN).

a. Kuota pengunaan data tidak ditentukan dikarenakan bersifat

bebas pakai oleh Kominfo Kota Palangka Raya menggunakan jaringan *Wifi.id* Telkom Indonesia (Penyedia layanan Internet).

b. Penyedia layanan internet *Wifi.id* tidak memberikan data pengguna, tetapi disini yang di analisis adalah pengunjung acak yang mengakses jaringan bebas pakai di sediakan oleh Kominfo Kota Palangka Raya.

c. Penulis mencoba mengidentifikasi keberadaan dan keamanan yang digunakan wifi target dengan menggunakan software Wireshark.

d. Setelah mengetahui keberadaan dan keamanan yang digunakan wifi target, penulis masuk untuk mendapatkan koneksi dengan wifi target.

e. Langkah pengujian keamanan, setelah mendapatkan koneksi dengan wifi target, penulis mencoba melakukan serangan Packet Sniffing terhadap wifi dan jaringan kabel dengan menggunakan software ettercap, serangan akan berhasil jika transfer data tidak dilindungi oleh keamanan seperti SSL, IPSec, WEP, WPA dan WPA2. Karena data yang didapat terenkripsi

DAFTAR PUSTAKA

Agung Nugroho (2012).“Analisa Keamanan Jaringan Wireless Local Area Network Dengan Access Point Tp-Link Wa500g”. Skripsi Program Studi Teknik Informatika Fakultas Komunikasi Dan Informatika Universitas Muhammadiyah Surakarta

Ayu Syifa Destiani (2015).“Analisis Protokol Keamanan Situ Unpas Dengan Menggunakan Sslstrip Dan Wireshark”. Skripsi Program Studi Teknik Informatika Fakultas Teknik Universitas Pasundan Bandung

Bayu Arie Nugroho (2012).“Analisis Keamanan Jaringan Pada Fasilitas Internet (Wifi) Terhadap Serangan Packet Sniffing”. Skripsi Skripsi Program Studi Informatika Fakultas Komunikasi Dan Informatika Universitas Muhammadiyah Surakarta

Gilang Kumala Dewi (2016). “Analisa Keamanan Jaringan Wireless Di Sekolah Menengah Al Firdaus”. Skripsi Program Studi Informatika Fakultas Komunikasi Dan Informatika Universitas Muhammadiyah Surakarta

Kadir. Abdul. (2003). Pengenalan Sistem Informasi. Yogyakarta: Andi Offset.
Harahap, Sofyan Syafri. 2015. Analisis Kritis atas Laporan Keuangan. Edisi 1-10. Jakarta: Rajawali Pers.

Kustanto dan Daniel T saputro, 2015. Belajar Jaringan Komputer Berbasis Mikrotik OS. Yogyakarta: Gava Media.

M. R. Kurniawan (2018). “Analisis Sistem Keamanan Wireless Local Area Network (Wlan) Pada Proses Tethering”. Jurnal Jurusan Teknik Elektro Universitas Riau

Sam, Arianto. 2008. Pengertian Fasilitas Belajar dan Jenisnya. Tersedia : http://sobatbaru.blogspot.com/2014/10/pengertian.fasilitas.belajar.htm. Diperoleh 25 November 2014.

Singh, K. U. (2014). LSB Audio Steganograpy Approach. ISO 9001:2008 Certified Journal, Volume 4, Issue 4, April 2014, ISSN 2250-2459.

Yuni Fitriani. 2020. “Analisis Pemanfaatan Teknologi Informasi Dalam Pembelajaran Jarak Jauh Di Tengah Pandemi Virus Corona Covid-19”.

LAMPIRAN

Lampiran 1. Surat Tugas

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp. 0536-3225515 Fax. 0536-3225515 Palangkaraya
email : humas@stmikplk.ac.id – website : www. stmikplk.ac.id

SURAT TUGAS
No.307/STMIK-C.1/AK/II/2021

Ketua Program Studi Sistem Informasi Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya menugaskan nama-nama tersebut di bawah ini :

1. Nama : Sam'ani, ST., M.Kom.
   NIK : 197703252005105
   Sebagai Pembimbing I dalam **Materi Penelitian dan Program**

2. Nama : Hafiz Riyadli, M.Kom.
   NIK : 198604042010103
   Sebagai Pembimbing II dalam **Format Penulisan**

Untuk membimbing Tugas Akhir Mahasiswa :

Nama	:	Liantoni
NIM	:	C1757201023
Judul Tugas Akhir	:	Analisis Keamanan Jaringan Publik Pada Fasilitas Sosial Di Kota Palangka Raya Menggunakan Wireshark
Berlaku s/d	:	24 Maret 2022

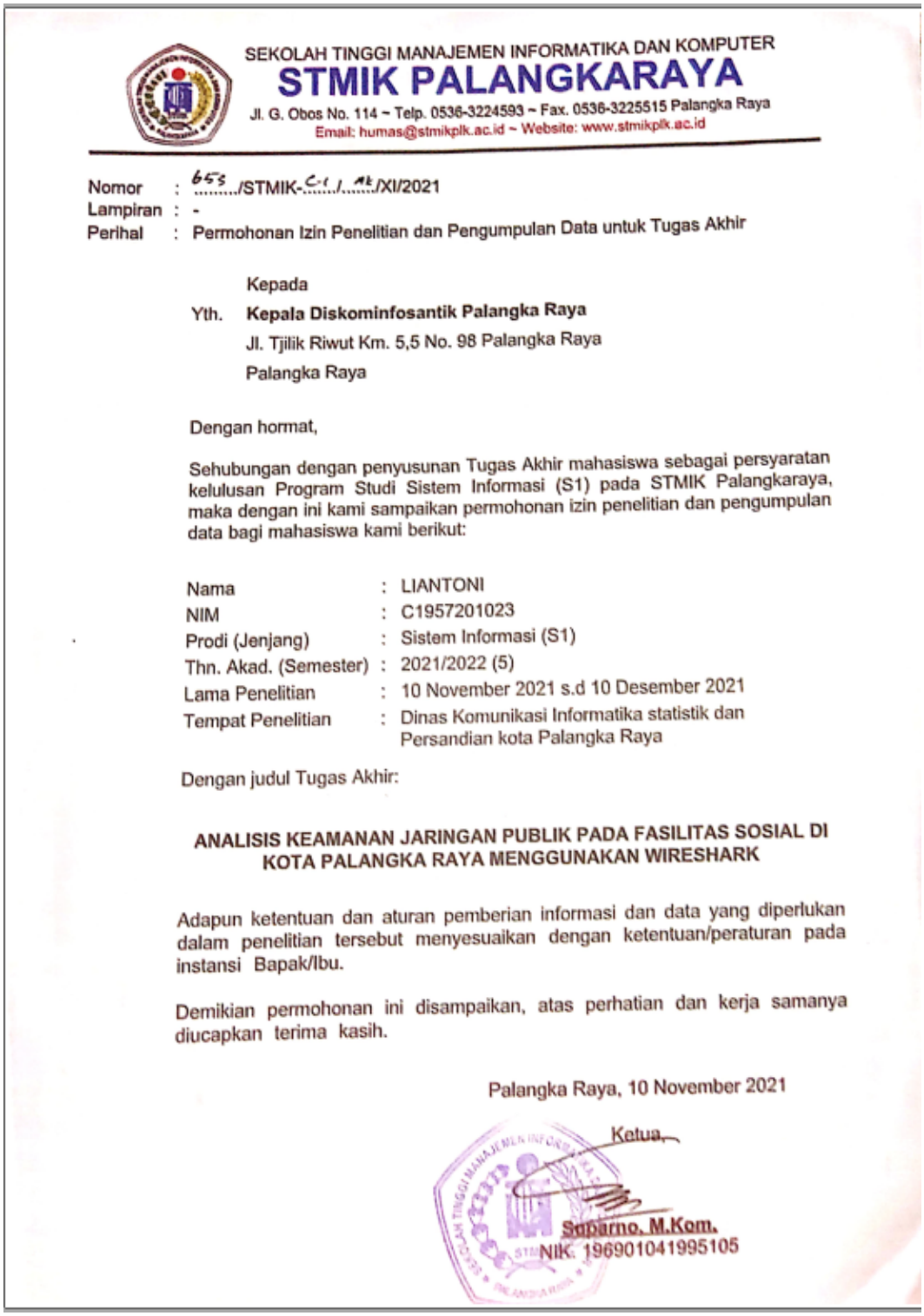
Demikian surat ini dibuat agar dapat dipergunakan sebagaimana mestinya dan dilaksanakan dengan penuh tanggung jawab.

Palangka Raya, 24 Maret 2021
Ketua Program Studi
Sistem Informasi

Norhayati, M.Pd.
NIK. 198805222011004

Tembusan :
1. Ketua STMIK Palangkaraya
2. Kepala Unit Penjaminan Mutu Internal (UPMI)
3. Dosen Pembimbing yang bersangkutan
4. Arsip Program studi Sistem Informasi

Lampiran 2. Surat Permohonan Izin Penelitian



SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
STMIK PALANGKARAYA
Jl. G. Obos No. 114 ~ Telp. 0536-3224593 ~ Fax. 0536-3225515 Palangka Raya
Email: humas@stmikplk.ac.id ~ Website: www.stmikplk.ac.id

Nomor : 655/STMIK-C-1/...../XI/2021
Lampiran : -
Perihal : Permohonan Izin Penelitian dan Pengumpulan Data untuk Tugas Akhir

Kepada
Yth. **Kepala Diskominfosantik Palangka Raya**
Jl. Tjilik Riwut Km. 5,5 No. 98 Palangka Raya
Palangka Raya

Dengan hormat,

Sehubungan dengan penyusunan Tugas Akhir mahasiswa sebagai persyaratan kelulusan Program Studi Sistem Informasi (S1) pada STMIK Palangkaraya, maka dengan ini kami sampaikan permohonan izin penelitian dan pengumpulan data bagi mahasiswa kami berikut:

Nama	:	LIANTONI
NIM	:	C1957201023
Prodi (Jenjang)	:	Sistem Informasi (S1)
Thn. Akad. (Semester)	:	2021/2022 (5)
Lama Penelitian	:	10 November 2021 s.d 10 Desember 2021
Tempat Penelitian	:	Dinas Komunikasi Informatika statistik dan Persandian kota Palangka Raya

Dengan judul Tugas Akhir:

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Adapun ketentuan dan aturan pemberian informasi dan data yang diperlukan dalam penelitian tersebut menyesuaikan dengan ketentuan/peraturan pada instansi Bapak/Ibu.

Demikian permohonan ini disampaikan, atas perhatian dan kerja samanya diucapkan terima kasih.

Palangka Raya, 10 November 2021

Ketua,

Saparno, M.Kom.
NIK. 196901041995105

Lampiran 3. Balasan Surat Izin Penelitian

PEMERINTAH KOTA PALANGKA RAYA
DINAS KOMUNIKASI, INFORMATIKA
STATISTIK DAN PERSANDIAN
Jl. Tjilik Riwut Km.5,5 No. 98 Palangka Raya
Website : www.palangkaraya.go.id

Palangka Raya, 29 November 2021

Nomor : 440/DKISP/XI/2021
Lampiran : -
Perihal : Pemberitahuan

Kepada,
Yth. Kepala STMIK Palangka Raya
Di-
Kota Palangka Raya

Sehubungan dengan pemintaan untuk izin penelitian mahasiswa atas nama :

Nama : LIANTONI

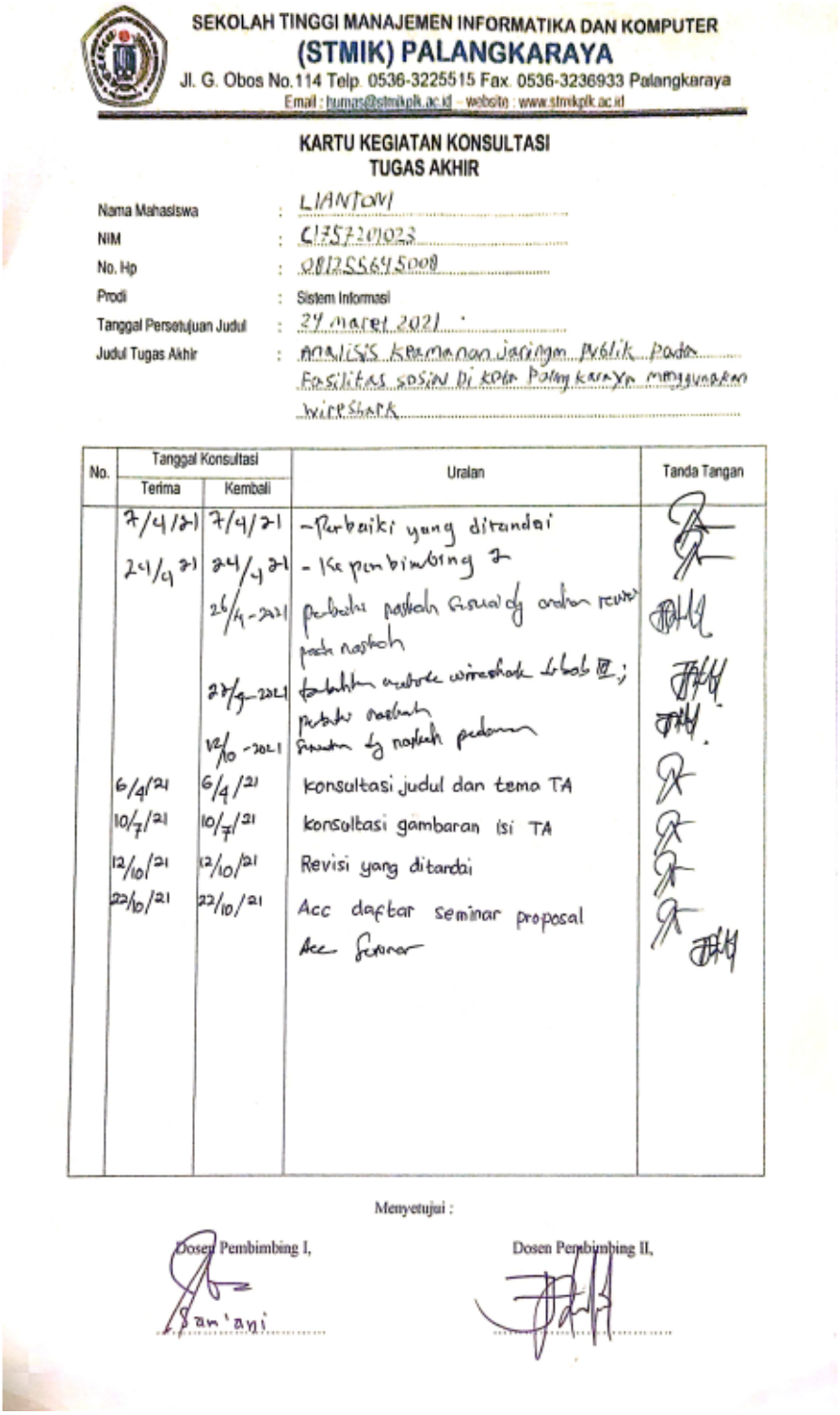
NIM : C1957201023

Demikian disampaikan dan dinyatakan mahasiswa tersebut di nyatakan telah melakukan penelitian dengan baik, atas perhatian dan kerjasamanya diucapkan terimakasih.

Plt. Kepala Dinas Komunikasi, Informatika, Statistik dan Persandian Kota Palangka Raya

Dra. FIFI ARFIANA, M.Si
Pembina Tingkat I
NIP. 19640704 198302 2 001

Lampiran 4. Kartu Kegiatan Konsultasi Tugas Akhir



SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp. 0536-3225515 Fax. 0536-3236933 Palangkaraya
E-mail : humas@stmikplk.ac.id – website : www.stmikplk.ac.id

KARTU KEGIATAN KONSULTASI
TUGAS AKHIR

Nama Mahasiswa : LIANTONI
NIM : C1757201023
No. Hp : 081255645008
Prodi : Sistem Informasi
Tanggal Persetujuan Judul : 29 maret 2021
Judul Tugas Akhir : analisis keamanan jaringan publik pada fasilitas sosial di kota palangkaraya menggunakan wireshark

No.	Tanggal Konsultasi		Uraian	Tanda Tangan
	Terima	Kembali		
	7/4/21	7/4/21	-Perbaiki yang ditandai	
	24/4/21	24/4/21	- Ke pembimbing 2	
		26/4-2021	perbaiki paskah sesuai dg arahan revisi pada naskah	
		27/5-2021	tambahkan contoke wireshark bab II ; perbaiki naskah	
		12/10-2021	lanjutkan bg naskah pedoman	
	6/4/21	6/4/21	konsultasi judul dan tema TA	
	10/7/21	10/7/21	konsultasi gambaran isi TA	
	12/10/21	12/10/21	Revisi yang ditandai	
	22/10/21	22/10/21	Acc daftar seminar proposal	
			Acc seminar	

Menyetujui :

Dosen Pembimbing I,

Sam'ani

Dosen Pembimbing II,

Lampiran 5. Kartu Kegiatan Seminar Proposal Tugas Akhir

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No 114 Telp 0536-3225515 Fax. 0536-3236933 Palangkaraya
Email : humas@stmikpk.ac.id – website : www.stmikpk.ac.id

KARTU KEGIATAN SEMINAR
PROPOSAL TUGAS AKHIR

Nama Mahasiswa : LIANTONI
NIM : C1J520023
Program Studi : Sistem Informasi

No.	Hari/ Tanggal	Judul	Mahasiswa Penyaji	Nama Tim Dosen	Tanda Tangan
1	Rabu, 20-01-2021	Aplikasi layanan laboratorium Online Bayi, karantina pemain kelas II Palangkaraya berbasis web Framework	Hardianto Tri Hartono	1. Ferdiyani Hanis, M.Kom 2. Rosmiaei, M.Kom 3. Sys. Herdarlie, M.Kom	
2	Rabu 22-01-2021	Implementasi Virtual Reality dalam pengenalan pelayanan kampus STMIK Palangka Raya	Juriatul Jannah	Sulistyowati, S.Kom, M.CS Herkules, S.Kom, M.CS Catharina, Z. M.Pd	
3.	Rabu 22-01-2021	penerapan teknologi Augmented Reality sebagai media promosi perumahan	ilyu wulan ndary	Tili Tuslina, M.Kom Sulistyowati, S.Kom, M.CS Rudini, M.Pd	
4.	Sabtu, 13-02-2021	Analisis dan desain media pembelajaran untuk anak Sekolah minggu GPdI Bukit Hiau berbasis android	Daud Bonyuah Ibrahim	1) Rosmiaei, M.Kom 2.) Bayu Protama Nugroho, S.Kom, MT 3. Sys. Herdarlie M.Kom	1.) 2.) 3.)
5.	Selasa, 16-03-2021	Sistem Informasi Pada "Keripik Ya! Ya!" berbasis web	muhammad vilary	1.) Fenroy Yedithia, S.Kom, M.TI. 2.) Ferdiyani Hanis, M.Kom 3.) Norhayati, M.Pd	1.) 2.) 3.)

Palangka Raya, ...
Mahasiswa ybs,

Keterangan :
- Harap kartu jangan sampai hilang, digunakan sebagai syarat seminar
- Minimal 5 (lima) kali mengikuti seminar

Lampiran 6. Jadwal Pennelitian

No	Kegiatan	Januari 2021-November 2021						
		Januari	Februari	Maret	Juli	Sept	Okto	Nov
1	Tahap Persiapan Penelitian							
a	Penyusunan Judul							
b	Pengajuan Judul							
c	Pengajuan Proposal							
2	Seminar Proposal							

Lampiran 7. Daftar Hadir Peserta Seminar Proposal Tugas Akhir

DAFTAR HADIR PESERTA
SEMINAR PROPOSAL SKRIPSI

1. Nama Penyaji : LANTONI
2. Hari/ Tanggal : Senin 08 - November 2021
3. Waktu : 12.00 WIB
4. Judul Proposal : Analisa keamanan jaringan publik / Pada Fasilitas Sosial di Kota Palangka Raya menggunakan WireShark

No.	Nama Mahasiswa	NIM	Tanda Tangan
1	JUNI MANUEL SEPTIN	C1672010085	
2	TULUS ARIS SUDIANTO	C1857201069	
3	DWI ARIYANTI	C1957 2010 24	
4	Wayan Wiyata	C1957201034	
5	PRAYOGO PANGESTU	C1857201001	
6	Septiani	C1857201035	
7	MIA AGUSSINTIYA.		
8	I KADEK WIDIHARTIKA	C1857201007	
9	Kristiana Nathalia	C1857201004	
10	Hendy Sukma	C1855201050	
11	Mery S. Tandiman	C1857201083	
12	Resta Novaliska	C1857201060	
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			

Palangka Raya, 08 November 2021

Mengetahui
Ketua Tim Penguji,

Mahasiswa Penyaji,