

**ANALISIS KEAMANAN JARINGAN (*WIFI*) TERHADAP  
SERANGAN *PACKET SNIFFING* DI KOS RONALDO**

**SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Informatika



disusun oleh

**BINTANG YOGA PRATAMA**

**16.11.0227**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2023**

**ANALISIS KEAMANAN JARINGAN (*WIFI*) TERHADAP  
SERANGAN *PACKET SNIFFING* DI KOS RONALDO**

**SKRIPSI**

untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Informatika



disusun oleh

**BINTANG YOGA PRATAMA**

**16.11.0227**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2023**

**HALAMAN PERSETUJUAN**

**SKRIPSI**

**ANALISIS KEAMANAN JARINGAN (*WIFI*) TERHADAP SERANGAN  
*PACKET SNIFFING* DI KOS RONALDO**

yang disusun dan diajukan oleh

**Bintang Yoga Pratama**

**16.11.0227**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 28 juli 2023

**Dosen Pembimbing,**



**Subektiningsih.M.Kom**

**NIK. 190302413**

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS KEAMANAN JARINGAN (*WIFI*) TERHADAP SERANGAN  
*PACKET SNIFFING* DI KOS RONALDO

yang disusun dan diajukan oleh

**Bintang Yoga Pratama**

16.11.0227

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 28 juli 2023

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Agit Amrullah, S.Kom., M.Kom  
NIK. 190302356



Anggit Ferdita Nugraha, S.T., M.Eng  
NIK. 190302480



Subektiningsih, M.Kom  
NIK. 190302413

Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 28 juli 2023

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom.  
NIK. 190302096

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini,

Nama mahasiswa : Bintang Yoga Pratama  
NIM : 16.11.0227

Menyatakan bahwa Skripsi dengan judul berikut:

**Analisis Keamanan Jaringan (*wifi*) Terhadap Serangan *Packet Sniffing* Di Kos Ronaldo**

Dosen Pembimbing : Subktiningsih,M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 28 juli 2023

Yang Menyatakan,



Bintang Yoga Pratama

## HALAMAN PERSEMBAHAN

Pertama-tama penulis ingin mengucapkan rasa syukur kepada Allah SWT atas nikmat yang diberikan-Nya, karena tanpa nikmat yang begitu banyak yang telah diberikan-Nya penulis tidak mungkin dapat menyelesaikan skripsi ini. Skripsi ini penulis persembahkan kepada orang tua yang telah mengisi dunia penulis dengan begitu banyak kebahagiaan yang tidak akan bisa dibayarkan walau hingga akhir zaman.



## KATA PENGANTAR

Alhamdulillah, dengan segala puji syukur penulis panjatkan kepada Allah SWT. Karena berkat nikmat-Nya penulis dapat menyelesaikan skripsi yang berjudul “*Analisis Keamanan Jaringan (Wifi) Terhadap Packet Sniffing Di Kos Ronaldo*”.

Skripsi ini disusun guna melengkapi salah satu syarat untuk memperoleh gelar Sarjana pada Jurusan Informatika Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta. Skripsi ini dibuat berdasarkan data yang penulis peroleh dari studi literatur, hasil percobaan maupun dari dosen pembimbing.

Penulis dapat menyelesaikan skripsi ini, tidak lepas dari bantuan beberapa pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih yang sebanyak-banyaknya kepada:

1. Allah SWT
2. Bapak Prof Dr M Suyanto, MM selaku Rektor Universitas AMIKOM Yogyakarta
3. Ibu Subektiningsih, M.Kom selaku dosen pembimbing skripsi yang telah memberikan waktu, arahan serta ilmunya selama membimbing penulis
4. Ibu Fitria Lahamang selaku ibu kandung yang selalu mendoakan, mengingatkan, menasihati, menyayangi, dan menyemangati penulis ketika sedang mengalami masalah
5. Bapak Harry Yudatama selaku ayah kandung dan Ibu Vera selaku ibu yang mendoakan, menasihati, dan menyayangi penulis
6. Adik Bima, Trias dan Rama selaku adik yang selalu mendoakan penulis
7. Galuh, Ervin, Nando, dan Malik selaku kerabat yang telah berbagi pengalaman kuliah dengan penulis

## DAFTAR ISI

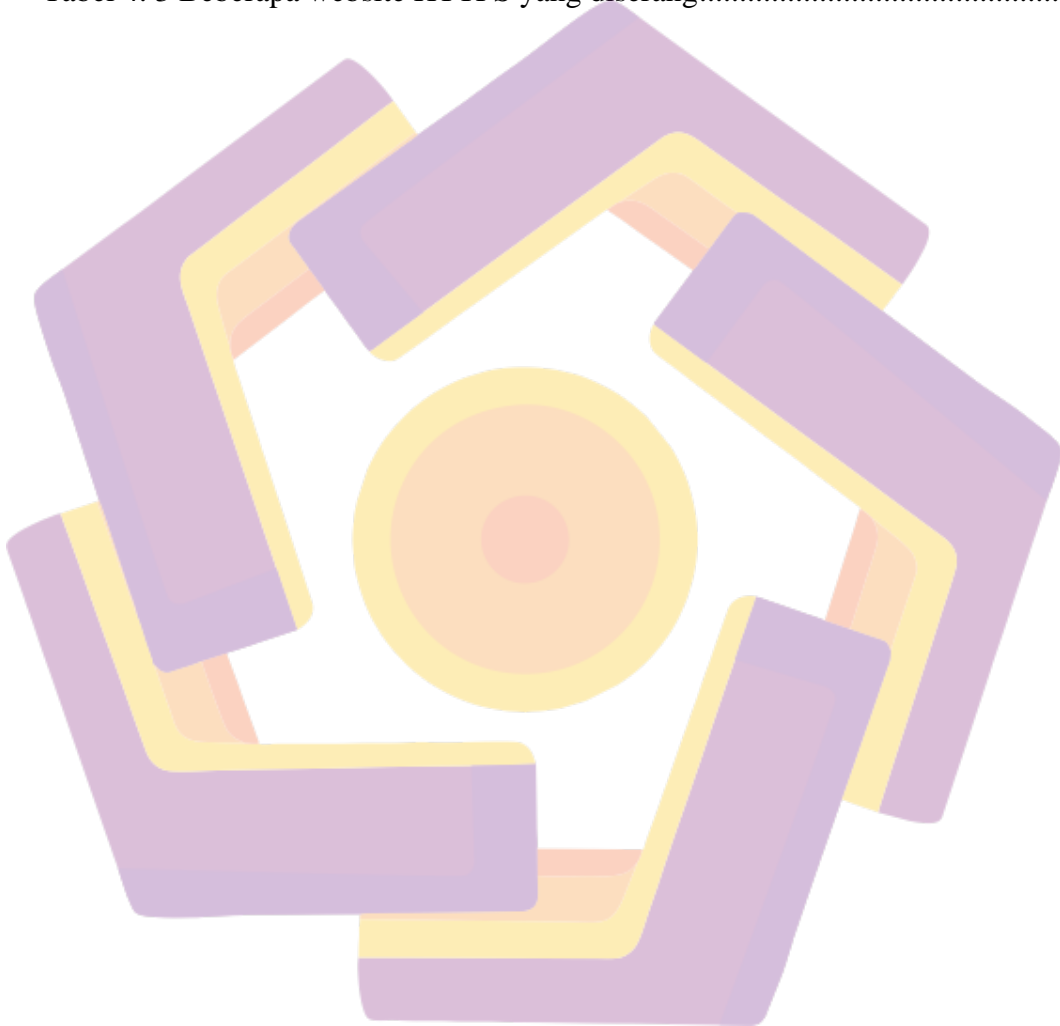
<b>HALAMAN JUDUL .....</b>	<b>i</b>
<b>HALAMAN PERSETUJUAN .....</b>	<b>ii</b>
<b>HALAMAN PENGESAHAN.....</b>	<b>ii</b>
<b>HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....</b>	<b>iii</b>
<b>HALAMAN PERSEMBAHAN .....</b>	<b>v</b>
<b>KATA PENGANTAR.....</b>	<b>vi</b>
<b>DAFTAR ISI.....</b>	<b>vii</b>
<b>DAFTAR TABEL .....</b>	<b>ix</b>
<b>DAFTAR GAMBAR.....</b>	<b>x</b>
<b>DAFTAR LAMPIRAN .....</b>	<b>xi</b>
<b>DAFTAR ISTILAH .....</b>	<b>xii</b>
<b>INTISARI .....</b>	<b>xiii</b>
<b>ABSTRACT .....</b>	<b>xiv</b>
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1 Latar Belakang Masalah .....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah .....	2
1.4 Tujuan Penelitian .....	2
1.5 Manfaat Penelitian .....	2
1.6 Sistematika Penulisan .....	3
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>4</b>
2.1 Studi Literatur .....	4
2.2 Konsep Dasar Internet .....	8
2.2.1 Pengertian Internet .....	8
2.2.2 Sejarah Internet .....	8
2.3 Konsep Dasar Protokol Internet.....	9



2.3.1	Pengertian Protokol Internet .....	9
2.3.1	TCP/IP .....	9
2.3.2	HTTP dan HTTPS .....	10
2.3	Konsep Dasar <i>Wifi</i> .....	12
2.4.1	Pengertian <i>Wifi</i> .....	12
2.4.2	Sejarah <i>Wifi</i> .....	12
2.4	<i>Packet Sniffing</i> .....	14
2.5.1	<i>Passive Sniffing</i> .....	14
2.5.2	<i>Active Sniffing</i> .....	14
2.6	<i>Arp Spoofing</i> .....	14
2.7	Wireshark.....	15
<b>BAB III METODE PENELITIAN .....</b>		<b>16</b>
3.1	Objek Penelitian.....	16
3.2	Alur Penelitian.....	18
3.2.1	Alat dan Bahan.....	20
3.2.1	Instalasi Perangkat Keras ( <i>hardware</i> ).....	21
3.2.2	Instalasi Perangkat Lunak ( <i>software</i> ).....	22
3.2.3	Tahapan-tahapan Penyerangan .....	22
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>		<b>27</b>
4.1	Simulasi Penyerangan.....	27
4.1.1	Penyerangan Terhadap <i>Website</i> HTTP .....	27
4.1.2	Penyerangan Terhadap <i>Website</i> HTTPS.....	32
4.2	Hasil Penelitian .....	34
4.3	Solusi Untuk Mencegah Serangan <i>Packet Sniffing</i> .....	35
4.4	Proses dan Hasil Diskusi.....	37
<b>BAB V KESIMPULAN DAN SARAN.....</b>		<b>39</b>
5.1	Kesimpulan .....	39
5.2	Saran .....	39
<b>REFERENSI.....</b>		<b>40</b>
<b>LAMPIRAN.....</b>		<b>42</b>

## DAFTAR TABEL

Tabel 2. 1 Keaslian Penelitian .....	6
Tabel 3. 1 Hardware yang akan digunakan.....	20
Tabel 3. 2 Software yang akan digunakan .....	21
Tabel 4. 2 Beberapa website HTTP yang diserang.....	31
Tabel 4. 3 Beberapa website HTTPS yang diserang.....	34



## DAFTAR GAMBAR

Gambar 2. 1 TCP/IP Layer .....	10
Gambar 2. 2 Logo Wifi .....	13
Gambar 3. 1 Hasil kuesioner keamanan wifi .....	16
Gambar 3. 2 Hasil kuesioner cyber crime .....	17
Gambar 3. 3 Hasil kuesioner keamanan website .....	17
Gambar 3. 4 Hasil kuesioner perbedaan http dan https .....	17
Gambar 3. 5 Hasil kuesioner login http .....	18
Gambar 3. 6 Hasil kuesioner login https .....	18
Gambar 3. 7 Flowchart Alur Penelitian .....	19
Gambar 3. 8 Tampilan Instalasi Aplikasi Wireshark .....	22
Gambar 3. 9 Flowchart Penyerangan Website HTTP .....	23
Gambar 3. 10 Flowchart Penyerangan Website HTTPS .....	25
Gambar 4. 1 Tampilan awal Ettercap .....	27
Gambar 4. 2 Proses scanning host & arp poisoning .....	28
Gambar 4. 3 Tampilan awal aplikasi Wireshark .....	28
Gambar 4. 4 Tampilan perekaman paket-paket .....	29
Gambar 4. 5 Aktivitas login pada website HTTP .....	29
Gambar 4. 6 Proses pemfilteran paket-paket HTTP .....	30
Gambar 4. 7 Tampilan isi paket yang menyimpan data login .....	30
Gambar 4. 8 Aktivitas login pada website HTTPS .....	32
Gambar 4. 9 Melakukan scanning ip address website .....	33
Gambar 4. 10 Proses pemfilteran paket-paket HTTPS .....	33
Gambar 4. 11 Setelan google chrome .....	35
Gambar 4. 12 Peringatan google chrome .....	36
Gambar 4. 13 Setelan Mozilla Firefox .....	36
Gambar 4. 14 Peringatan mozilla firefox .....	37
Gambar 4. 15 Proses Diskusi .....	38
Gambar 4. 16 Hasil Diskusi .....	38

## DAFTAR LAMPIRAN

Lampiran 1 Hasil Kuesioner .....	42
----------------------------------	----



## DAFTAR ISTILAH



ARP	: <i>Address Resolution Protocol</i>
DNS	: <i>Domain Name System</i>
HTML	: <i>HyperText Markup Language</i>
HTTP	: <i>HyperText Transfer Protocol</i>
HTTPS	: <i>HyperText Transfer Protocol Secure</i>
IBM	: <i>International Business Machines</i>
IEEE	: <i>Institute of Electrical and Electronics Engineers</i>
INTERNET	: <i>Interconnected Network</i>
IP	: <i>Internet Protocol</i>
ISP	: <i>Internet Service Provider</i>
LAN	: <i>Local Area Network</i>
MAC	: <i>Media Access Control</i>
MIMO	: <i>Multiple-Input Multiple-Output</i>
MITM	: <i>Man in The Middle</i>
PDA	: <i>Personal Digital Assistant</i>
RF	: <i>Radio Frequency</i>
SSL	: <i>Secure Socket Layer</i>
TCP	: <i>Transmission Control Protocol</i>
TLS	: <i>Transport Layer Security</i>
UDP	: <i>User Data Protocol</i>
WAN	: <i>Wide Area Network</i>
WIFI	: <i>Wireless Fidelity</i>
WPA2-PSK	: <i>Wi-Fi Protected Access 2 – Pre-Shared Key</i>

## INTISARI

Internet menjadi salah satu kebutuhan utama bagi beberapa orang, karena internet dapat membantu di beberapa bidang seperti kesehatan, pendidikan bisnis dan lainnya. Membuat keamanan jaringan internet menjadi sebuah aspek yang wajib diperhatikan, jaringan internet sangat rentan terhadap serangan-serangan yang dilakukan oleh *hacker*. Salah satu serangannya adalah *packet sniffing*, dimana pelaku atau *hacker* dapat melihat data-data yang kita kirim maupun data yang akan kita terima dan bahkan dapat merubah isi data-data tersebut.

Dengan menggunakan metode penelitian eksperimen dan teknik pengumpulan data wawancara dan kuesioner untuk mendapatkan data yang berkaitan dengan penelitian. Solusi untuk masalah ini adalah dengan menganalisis kinerja jaringan komputer itu sendiri menggunakan beberapa aplikasi *Network Analyzer*. Dalam kasus kali ini, penulis menggunakan aplikasi *Wireshark*, dan menguji coba dengan cara melakukan penyerangan *packet sniffing* untuk membuktikan keamanan jaringan (*Wifi*) yang ada di Kos Ronaldo.

Hasil penelitian menunjukkan bahwa, uji coba serangan *packet sniffing* berhasil dilakukan jika korban menggunakan atau mengakses *website* yang menggunakan protokol *http*. Sedangkan uji serangan pada *website* yang menggunakan protokol *https* tidak berhasil mendapatkan hasil.

**Kata kunci:** keamanan jaringan, *packet sniffing*, *wireshark*

## ABSTRACT

*The internet is one of the main needs for some people, because the internet can help in several fields such as health, business education and others. Making internet network security an aspect that must be considered, internet networks are very vulnerable to attacks carried out by hackers. One of the attacks is packet sniffing, where the perpetrator or hacker can see the data that we send and the data that we will receive and can even change the contents of the data.*

*By using experimental research methods and data collection techniques interviews and questionnaires to obtain data related to research. The solution to this problem is to analyze the performance of the computer network itself using several Network Analyzer applications. In this case, the author uses the Wireshark application, and tests it by carrying out a packet sniffing attack to prove network security (Wifi) at Kos Ronaldo.*

*The results of the study show that the trial packet sniffing attack is successful if the victim uses or accesses a website that uses the http protocol. Meanwhile, the attack test on websites using the https protocol failed to get results.*

*Keyword: network security, packet sniffing, wireshark*

