EVALUASI KAPABILITAS DETEKSI ANTI-SPYWARE TERHADAP PACKER SPYWARE MODE STEALTH

Proposal Tugas Akhir

Oleh

Nathaniel Liady
18222114

PROGRAM STUDI SISTEM DAN TEKNOLOGI INFORMASI
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG

November 2025

LEMBAR PENGESAHAN

EVALUASI KAPABILITAS DETEKSI ANTI-SPYWARE TERHADAP PACKER SPYWARE MODE STEALTH

Proposal Tugas Akhir

Oleh

Nathaniel Liady
18222114

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Proposal Tugas Akhir ini telah disetujui dan disahkan
di Bandung, pada tanggal 30 November 2025

Pembimbing

Prof. Dr. Ir. Suhardi, M.T.

NIP. 123456789

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR KODE

II.1 Contoh pseudocode 15
II.2 Contoh source code Python 15

BAB I

PENDAHULUAN

I.1 Latar Belakang

Ancaman siber saat ini telah berevolusi dari malware tradisional berbasis file menjadi serangan yang lebih canggih dan tersembunyi, seperti fileless *malware* dan *spyware*. Malware jenis ini dirancang khusus untuk menghindari deteksi dengan memanfaatkan fitur-fitur sah dari sistem operasi, seperti PowerShell dan Windows Management Instrumentation (WMI), untuk menjalankan kode berbahaya langsung di memori tanpa menulis file apapun ke disk. Karena tidak memiliki file yang dapat dideteksi oleh *antivirus* berbasis tanda tangan (signature-based), serangan ini seringkali luput dari pantauan sistem keamanan tradisional.

Kecanggihan ini membuat fileless malware menjadi ancaman yang sangat berbahaya bagi perusahaan manapun karena kemampuannya untuk bertahan lama dan menghindari solusi *antivirus* yang ada. Menurut penelitian, *anti-spyware* modern masih memiliki kelemahan signifikan, bahkan terhadap malware ”lama” yang dimodifikasi dengan trik baru. Misalnya, sebuah studi pada tahun 2023 menemukan bahwa hampir separuh dari 12 mesin *antivirus* yang diuji hanya mampu mendeteksi kurang dari setengah varian malware yang disamarkan. Penelitian lain juga menunjukkan bahwa metode seperti enkripsi, injeksi proses, dan penambahan data sampah ke file eksekusi (*junk data*) terbukti sangat efektif dalam menghindari deteksi. Teknik ini bahkan dapat membingungkan *antivirus* gratis dan berbayar, membuat mereka gagal mendeteksi atau mengkarantina file yang berbahaya.

Situasi ini semakin diperparah dengan temuan bahwa banyak alat keamanan, termasuk *anti-spyware*, sering kali gagal menganalisis kode yang dikemas menggunakan alat populer seperti PyInstaller untuk bahasa *Python*. Hal ini terjadi karena *antivirus* tidak dapat memahami konten kode bita *Python (Python bytecode)*, yang secara efektif menyamarkan skrip berbahaya dari analisis statis. Kurangnya deteksi yang

efektif oleh solusi keamanan yang ada, termasuk *anti-spyware* dan EDRs (*Endpoint Detection and Response*), menciptakan celah besar yang dieksploitasi oleh kelompok penjahat siber dan APTs (*Advanced Persistent Threats*), yang semakin sering menggunakan skrip *fileless PowerShell* untuk menghindari pertahanan.

I.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana kapabilitas sistem *anti-spyware* dalam mendeteksi aktivitas tersembunyi dari perilaku *spyware mode stealth* pada lingkungan uji terkontrol?
2. Bagaimana pendekatan paling efektif untuk menyisipkan *spyware mode stealth* ke sistem?
3. Bagaimana teknik penyamaran (obfuscation) dan metode eksekusi berbasis memori (in-memory execution) mempengaruhi kemampuan deteksi produk *anti-spyware* saat ini?
4. Apa saja celah keamanan dan kelemahan spesifik yang ditemukan pada produk *anti-spyware* dan EDR ketika dihadapkan pada serangan spyware kustom yang dirancang untuk menghindari deteksi?

I.3 Tujuan

Secara umum, tujuan dari pelaksanaan tugas akhir ini adalah untuk mengukur dan mengevaluasi efektivitas produk *anti-spyware* dan EDR komersial dalam mendeteksi *spyware mode stealth* yang dikembangkan dengan teknik-teknik penghindaran deteksi modern.

Secara spesifik, tujuan yang ingin dicapai adalah:

1. Menganalisis dan mengidentifikasi teknik-teknik evasi yang paling efektif digunakan oleh *spyware* untuk menghindari deteksi dari *anti-spyware* dan EDR.
2. Mengembangkan sebuah prototipe *spyware mode stealth*, termasuk *reverse shell fileless PowerShell*, yang menggabungkan teknik-teknik evasif yang telah diidentifikasi.
3. Melakukan pengujian komparatif prototipe *spyware* pada sejumlah produk *anti-spyware* dan EDR komersial untuk mengevaluasi tingkat keberhasilan dan kegagalan deteksi.
4. Mendokumentasikan dan mempublikasikan celah keamanan yang ditemukan pada produk *anti-spyware*, serta menyusun rekomendasi mitigasi untuk pe-

ngembangan sistem pertahanan yang lebih adaptif dan tangguh.

kriteria keberhasilan dari pelaksanaan tugas akhir ini adalah:

- Prototipe *spyware* berhasil dikembangkan dengan setidaknya dua teknik evasif (misalnya, enkripsi dan obfuscation) dan mampu menghindari deteksi oleh salah satu produk *anti-spyware* yang diuji.
- Hasil pengujian menunjukkan bahwa ada perbedaan signifikan dalam tingkat deteksi antara format skrip dan *anti-spyware* yang berbeda.

Kedua kriteria tersebut menjadi indikator utama untuk menilai efektivitas penelitian, serta menunjukkan sejauh mana solusi yang ditawarkan mampu mengungkap kelemahan sistem keamanan siber saat ini. Pencapaian terhadap kriteria ini diharapkan dapat menjadi dasar pertimbangan dalam peningkatan kapabilitas deteksi *anti-spyware* dan EDR di masa depan

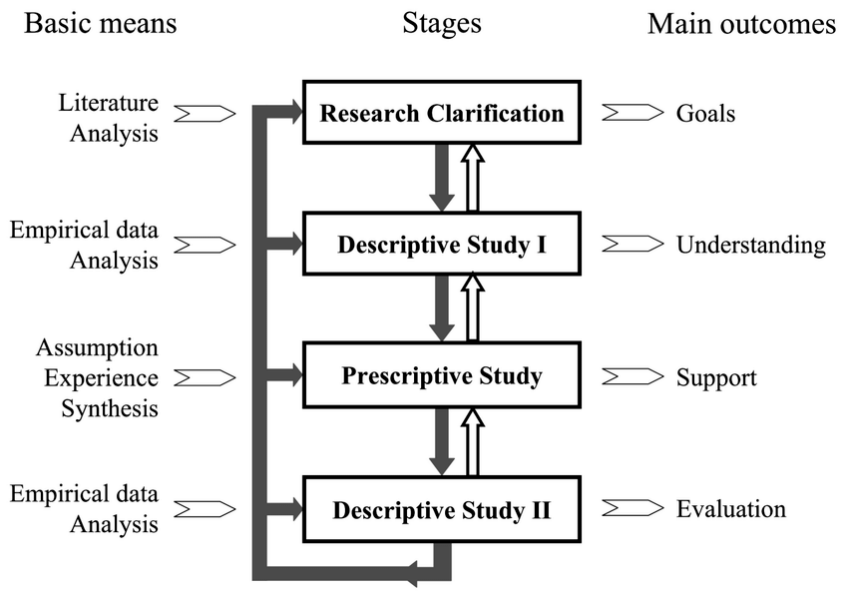
I.4 Batasan Masalah

Batasan masalah dalam pelaksanaan tugas akhir adalah sebagai berikut:

1. Penelitian ini hanya berfokus pada pengujian kapabilitas deteksi *anti-spyware* terhadap aktivitas awal (*Initial Access*) yang dilakukan oleh *spyware mode stealth* pada sistem operasi *desktop*.
2. Evaluasi hanya mencakup perangkat anti *spyware* yang dipilih sesuai kriteria penelitian, tidak membandingkan seluruh produk anti malware yang ada.
3. Aktivitas *malware* yang diujikan dibatasi secara ketat pada tahap penyusupan, enkripsi *payload*, *fileless execution*, dan upaya *persistence*.
4. Tugas akhir ini dikerjakan secara kelompok dengan anggota penelitian sebagai berikut:
    - Nathaniel Liady
    - M. Kasyfil Aziz
    - Audra Zelvania Putri Harjanto
    - Khayla Belva Annandira

I.5 Metodologi

Metodologi penelitian yang digunakan adalah *Design Research Methodology* (DRM) dikenalkan oleh (**Blessing2009DesignResearchMethodology**). DRM dibuat dengan tujuan supaya riset dilakukan dengan lebih efektif dan efisien. Metodologi ini terdiri dari empat tahap utama yaitu Research Clarification (RC), Descriptive Study I (DS-I), Perspective Study (PS), dan Descriptive Study II (DS-II). Berikut ini adalah gambaran dari kerangka kerja DRM.



Gambar 1.1 *Design Research Methodology* Framework

(a) *Research Clarification (RC)*

Fase ini akan dimulai dengan identifikasi masalah utama: adanya celah yang signifikan antara teknik serangan siber modern, khususnya *spyware mode stealth*, dan kemampuan deteksi solusi keamanan yang ada. Pengumpulan data awal akan dilakukan melalui tinjauan literatur komprehensif, termasuk laporan industri, artikel akademis, dan berita, untuk memahami lanskap ancaman dan teknik evasif yang digunakan untuk menghindari deteksi *anti-spyware* dan EDR. Hasil dari fase ini adalah rumusan masalah yang jelas dan terperinci, yang akan menjadi landasan untuk seluruh penelitian.

(b) *Descriptive Study I (DS-I)*

Pada fase ini, analisis mendalam terhadap masalah yang telah dirumuskan akan dilakukan dengan mengumpulkan data dan informasi yang relevan. Ini mencakup analisis rinci mengenai teknik-teknik evasi canggih, seperti penggunaan *PowerShell* dan obfuscation, untuk memahami bagaimana ancaman ini bekerja dan mengapa mereka sulit dideteksi. Selain itu, studi-studi terdahulu yang telah menguji bypass *antivirus* akan dikaji untuk mendapatkan wawasan mengenai metode dan potensi hasil. Sebagai bagian penting dari fase ini, alur kerja atau arsitektur teknis dari serangan *spyware* akan disusun, yang akan menjelaskan fase-fase seperti *Initial Access, Establish Foothold, Persistence, Data Collection*, dan *Exfiltration*. Diagram alur yang telah ada akan menjadi representasi visual dari arsitektur ini.

(c) *Perspective Study (PS)*

Fase ini merupakan inti dari DRM, di mana solusi untuk masalah yang telah didefinisikan akan dirancang dan dikembangkan. Artefak yang akan dibuat adalah prototipe *spyware mode stealth* dengan fungsi-fungsi spesifik seperti *keylogging* dan *screen capture*. Desain prototipe akan mengintegrasikan teknik evasi yang telah diidentifikasi pada fase sebelumnya, seperti enkripsi *payload* dan penggunaan PowerShell untuk menjalankan kode langsung di memori. Berbagai modul, termasuk Packer untuk menyamarkan *payload*.

(d) *Descriptive Study II (DS-II)*

Fase terakhir ini bertujuan untuk menguji dan mengevaluasi efektivitas solusi yang telah dikembangkan. Serangkaian pengujian eksperimental akan dilakukan dalam lingkungan virtual yang terisolasi untuk mengukur tingkat deteksi berbagai produk *anti-spyware* terhadap prototipe *spyware*. Hasil pengujian akan dianalisis untuk mengidentifikasi teknik evasi mana yang paling efektif dan mengapa produk keamanan tertentu gagal atau berhasil dalam mendeteksi ancaman. Analisis ini akan memvalidasi temuan awal dan memberikan kontribusi nyata pada pemahaman tentang kerentanan sistem keamanan modern, yang akan menjadi dasar untuk rekomendasi perbaikan dan penelitian lebih lanjut.

BAB II
STUDI LITERATUR

Bab ini membahas landasan teori dan kajian literatur yang relevan untuk mendukung penelitian ini. Studi literatur dilakukan untuk memahami konsep, teori, dan teknologi yang mendasari penelitian, termasuk *information gathering, social engineering, cyber security, anti-malware, malware*, dan *spyware*. Selain itu, kajian terhadap penelitian terdahulu yang berkaitan juga dilakukan untuk mengidentifikasi solusi yang sudah ada, celah penelitian, serta pendekatan yang dapat diadopsi atau dikembangkan lebih lanjut. Hasil dari studi literatur ini akan menjadi dasar dalam merumuskan solusi desain yang diusulkan dalam penelitian ini.

II.1 *Information Gathering*

Information gathering merupakan tahap awal yang sangat penting dalam proses pengujian keamanan siber maupun kegiatan intelijen digital. Tahap ini bertujuan untuk mengumpulkan informasi sebanyak mungkin mengenai target, baik berupa sistem, jaringan, organisasi, maupun individu, dengan tujuan memahami permukaan serangan yang tersedia. (**Verma2021InformationGathering**) menjelaskan bahwa kegiatan *information gathering* dilakukan untuk memetakan aset dan mengidentifikasi potensi kerentanan sebelum serangan atau pengujian keamanan dilakukan. Secara umum, proses ini terbagi menjadi dua pendekatan utama, yaitu pasif dan aktif. Pengumpulan informasi secara pasif dilakukan tanpa melakukan interaksi langsung dengan sistem target, misalnya dengan memanfaatkan data publik dari mesin pencari, basis data domain, atau sumber intelijen terbuka (*Open Source Intelligence/OSINT*). Sebaliknya, pendekatan aktif melibatkan aktivitas langsung seperti *port scanning, service enumeration*, atau *banner grabbing* untuk memperoleh data teknis yang lebih spesifik, namun metode ini berisiko lebih tinggi untuk terdeteksi oleh sistem keamanan target.

Teknik *information gathering* secara tradisional terdiri atas tiga tahap utama,

yaitu *footprinting, scanning*, dan *enumeration*. Pada tahap *footprinting*, peneliti mengumpulkan informasi dasar seperti alamat IP, nama domain, sistem operasi, serta teknologi yang digunakan. Tahap *scanning* bertujuan untuk menemukan *host* aktif dan *port* terbuka, sementara *enumeration* melibatkan eksplorasi lebih dalam terhadap layanan, pengguna, atau konfigurasi sistem yang dapat dimanfaatkan dalam tahap berikutnya. Seiring berkembangnya teknologi, berbagai alat bantu seperti Nmap, Wireshark, The Harvester, Netcraft, dan Metagoofil banyak digunakan untuk mendukung proses pengumpulan informasi ini. Studi (**Verma2021InformationGathering**) juga menyoroti pentingnya kombinasi antara OSINT dan pemindaian aktif untuk meningkatkan efektivitas deteksi potensi risiko, meskipun penggunaan metode ini harus dibatasi dalam ruang lingkup yang legal dan etis.

Selain aspek teknis, penelitian terbaru menekankan pentingnya aspek etika dan hukum dalam kegiatan *information gathering*. Pengumpulan data secara berlebihan atau tanpa izin dapat melanggar privasi individu maupun regulasi keamanan informasi. Oleh karena itu, para peneliti dianjurkan untuk melakukan kegiatan ini dalam lingkungan laboratorium yang terisolasi, dengan batasan yang jelas dan persetujuan dari pihak terkait. Di sisi lain, hasil pengumpulan informasi juga harus dikelola dengan prinsip *responsible disclosure*, yaitu melaporkan temuan yang berpotensi sensitif kepada pihak yang berwenang tanpa menyebarkannya secara publik. Dengan demikian, *information gathering* tidak hanya berfungsi sebagai tahapan teknis untuk mendukung pengujian keamanan, tetapi juga sebagai fondasi penting dalam membangun kesadaran, kebijakan, dan strategi pertahanan siber yang lebih komprehensif.

II.2 *Social Engineering*

Social engineering adalah teknik manipulasi psikologis yang mengeksploitasi kelemahan manusia, bukan kerentanan teknis pada sistem keamanan. Dalam lanskap siber yang terus berkembang, *social engineering* menjadi salah satu ancaman paling signifikan dan efektif. Sejak tahun 2021, serangan *social engineering* telah meningkat baik dari segi volume maupun kecanggihan, dengan penjahat siber dan kelompok terorganisir mengeksploitasi bias kognitif dan emosi manusia untuk menipu. Ini menjadikan faktor manusia sebagai mata rantai terlemah dalam keamanan siber

Penelitian terbaru mengidentifikasi berbagai metode serangan *social engineering*, mulai dari yang sederhana hingga yang sangat canggih. *Phishing, spear phishing*, dan *whaling* adalah serangan yang menggunakan email atau pes-

an palsu yang disesuaikan untuk menipu individu atau target tingkat tinggi. Serangan *phishing* di media sosial juga dapat menjangkau audiens yang lebih luas daripada email konvensional. Selain itu, *pretexting* adalah ketika penyerang menciptakan skenario palsu untuk mendapatkan informasi sensitif atau akses, sering kali dengan menyamar sebagai rekan kerja atau figur otoritas. Ada juga metode *baiting* yang menggunakan umpan (seperti file berbahaya) atau manipulasi suara untuk memancing korban agar mengambil tindakan yang membahayakan. Penyerang juga dapat melakukan *impersonation*, yaitu menyamar sebagai individu yang dikenal atau dipercaya, sebuah taktik yang lebih mudah dilakukan di media sosial karena melimpahnya informasi korban. Untuk meningkatkan presisi dan skalabilitas, penjahat siber kini juga memanfaatkan teknologi canggih seperti kecerdasan buatan (AI) dan *deepfake* untuk membuat serangan *social engineering* lebih meyakinkan.
Berbagai studi telah mengidentifikasi beberapa faktor yang membuat individu rentan terhadap serangan *social engineering*. Kesadaran keamanan yang rendah adalah salah satu faktor utama. Penyerang juga mengeksploitasi emosi seperti ketakutan, urgensi, rasa ingin tahu, dan kepercayaan untuk mendorong korban membuat keputusan yang salah. Kepercayaan berlebihan pada figur otoritas juga membuat korban lebih mudah dimanipulasi. Serangan-serangan ini memiliki dampak yang signifikan, termasuk kerugian finansial, kerusakan reputasi, dan hilangnya data. Studi kasus skema penipuan keuangan yang menargetkan Google dan Facebook menunjukkan bahwa organisasi dengan sistem keamanan yang kuat pun tidak kebal terhadap *social engineering*.

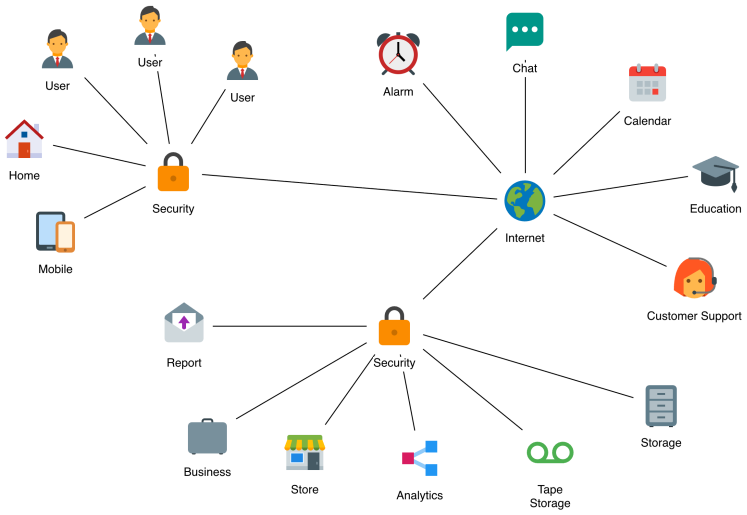
II.3 *Cyber Security*

Cyber security merupakan disiplin ilmu dan praktik yang berfokus pada perlindungan sistem komputer, jaringan, data, serta perangkat digital dari berbagai ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Menurut (**Ainslie2023CTI**), keamanan siber tidak hanya menjadi isu teknis, melainkan juga tantangan strategis yang berpengaruh terhadap pengambilan keputusan di tingkat organisasi. Dalam konteks modern, setiap keputusan bisnis harus mempertimbangkan potensi risiko siber, karena ancaman digital kini dapat berdampak langsung pada keberlanjutan operasional dan reputasi perusahaan. Oleh karena itu, *cyber security* mencakup kombinasi aspek teknologi, manusia, dan kebijakan organisasi yang bekerja secara terpadu untuk mencegah, mendeteksi, dan merespons insiden keamanan secara efektif.

Komponen utama dalam *cyber security* meliputi perlindungan data dan privasi, pengelolaan risiko, deteksi serta respons terhadap insiden, hingga penerapan *Cyber Threat Intelligence (CTI)* yang berfungsi untuk mengidentifikasi pola serangan dan memberikan wawasan bagi pengambilan keputusan keamanan (**Ainslie2023CTI**). Selain itu, munculnya ancaman baru seperti fileless malware turut memperluas ruang lingkup keamanan siber. Berdasarkan penelitian (**Sudhakar2020FilelessMalware**), *fileless malware* beroperasi langsung di memori tanpa menyimpan file berbahaya di sistem, sehingga sulit dideteksi oleh *antivirus* tradisional yang berbasis tanda tangan. Ancaman ini menunjukkan bahwa sistem pertahanan harus bergeser dari deteksi berbasis file menuju pendekatan berbasis perilaku dan analisis memori.
Dalam penerapannya, pendekatan holistik menjadi kunci keberhasilan manajemen keamanan siber. FLECO, sebuah kerangka kerja yang dikembangkan oleh (**DominguezDorado2024FLECO**), menekankan pentingnya integrasi antara aspek teknologi, tata kelola, dan budaya organisasi untuk membangun sistem keamanan yang berkelanjutan. Pendekatan ini membantu organisasi dalam mengukur kesiapan keamanan siber dan memperkuat koordinasi lintas departemen agar setiap unit memahami tanggung jawabnya dalam menjaga keamanan digital. Dengan demikian, *cyber security* tidak hanya berfungsi untuk merespons ancaman yang terjadi, tetapi juga sebagai strategi proaktif yang melibatkan seluruh komponen organisasi dalam menciptakan ketahanan siber yang adaptif dan menyeluruh.

II.4 *Anto-Malware*

Anti-malware merupakan salah satu komponen inti dalam sistem pertahanan siber yang dirancang untuk mendeteksi, mencegah, dan menanggulangi perangkat lunak berbahaya seperti virus, trojan, *ransomware*, maupun *spyware*. Seiring berkembangnya kompleksitas serangan dan munculnya varian malware yang memanfaatkan teknik penyamaran (*obfuscation*), efektivitas sistem deteksi tradisional berbasis tanda tangan mengalami penurunan signifikan. Menurut Tayyab dkk. (2022), pendekatan modern dalam deteksi malware harus menggabungkan analisis statis dan dinamis untuk meningkatkan kemampuan identifikasi terhadap ancaman baru. Melalui penerapan deep learning berbasis analisis perilaku, penelitian mereka menunjukkan peningkatan akurasi deteksi hingga lebih dari 97%, menegaskan bahwa integrasi metode pembelajaran mesin dan analisis perilaku jauh lebih efisien dibanding deteksi berbasis pola semata.



Gambar II.1 Contoh gambar jaringan

II.4.1 Gambar

Contoh gambar dapat dilihat pada Gambar **??**. Gambar dan judulnya diposisikan di tengah. Nomor gambar tidak diakhiri tanda titik. Gambar tersebut dibuat menggunakan aplikasi draw.io dan disimpan ke format PNG setelah dengan zoom setting pada angka 300%. Ukuran gambar yang ditampilkan dapat diatur dengan mengubah nilai *width* dalam sintaks *includegraphics*.
Gambar umumnya tidak jelas atau kabur jika gambar tersebut:

a. diperoleh dari hasil cropping pada suatu halaman buku atau situs web;
b. hasil pembesaran gambar yang gambar aslinya sebenarnya berukuran kecil; atau
c. disimpan dalam resolusi kecil.

Ketidakjelasan gambar ini dapat dilihat pada garis-garis diagram yang tidak tegas dan tulisan-tulisan dalam gambar yang tampak kabur dan kurang jelas terbaca.
Untuk mendapatkan gambar yang tidak kabur (*blur*), langkah-langkah berikut dapat digunakan:

(a) Gambar yang didapat di suatu pustaka atau referensi sebaiknya digambar ulang, misalnya menggunakan PowerPoint, Canva, Figma, draw.io, atau yang lainnya.
(b) Jika diagram atau ilustrasi digambar menggunakan draw.io, saat gambar disimpan ke format PNG atau JPG (*export as*), lakukan *zoom* ke minimal 300% (*the default value is* 100%).
(c) Jika diagram digambar dengan menggunakan PowerPoint, gambar dapat langsung di-*copy-paste* ke Word.

Tabel II.1 Tabel harga bahan pokok

Nama	Satuan	Harga
Buku	Exemplar	25000
Komputer	Unit	2500000
Pensil	Buah	118900

Tabel II.2 Tabel harga bahan sekunder

Nama	Satuan	Harga
Buku	Exemplar	25000
Komputer	Unit	2500000
Pensil	Buah	118900

II.4.2 Tabel

Tabel ada dua jenis, yaitu tabel yang bisa termuat dalam satu halaman dan tabel yang sangat panjang sehingga tidak muat dalam satu halaman.

II.4.2.1 Tabel yang Muat dalam Satu Halaman

Contoh tabel dapat dilihat pada Tabel **??** dan **??**. Tabel dan judulnya dibuat rata kiri dan judul tabel diletakkan di atas tabel. Usahakan tabel dapat ditulis dalam satu halaman, tidak terpotong ke halaman berikutnya.

II.4.2.2 Mengimpor Tabel dari Berkas Eksternal

Tabel **??** diimpor dari berkas eksternal *table/tabel1.tex* menggunakan perintah *input*. Dengan demikian, jika tabel tersebut perlu diubah, cukup mengubah pada berkas eksternal tersebut tanpa perlu mengubah pada berkas utama ini.

Tabel II.3 Tabel harga bahan tertier

Nama	Satuan	Harga
Buku	Exemplar	25000
Komputer	Unit	2500000
Pensil	Buah	118900
Pensil	Buah	118900
Pensil	Buah	118900
Pensil	Buah	118900
Pensil	Buah	118900

II.4.2.3 Tabel yang Sangat Panjang

Jika tabel terlalu panjang sehingga tidak muat dalam satu halaman, gunakan paket *longtable* untuk membuat tabel yang dapat terpotong ke halaman berikutnya, seperti pada Tabel **??**.

Tabel II.4 Comprehensive Data Table Example

	ID	Name	Score	Rank
1		Alice Smith	89	5
2		Bob Johnson	93	3
3		Carol Davis	95	2
4		Daniel Wilson	88	6
5		Eve Thompson	97	1
6		Frank Brown	85	7
7		Grace Lee	91	4
8		Henry Miller	80	9
9		Irene Garcia	83	8
10		Jack Robinson	78	10
11		Kevin Harris	76	11
12		Laura Martin	75	12
13		Michael Clark	74	13
14		Natalie Lewis	73	14
15		Olivia Walker	72	15
16		Peter Hall	71	16
17		Quinn Allen	70	17
18		Rachel Young	69	18
19		Samuel King	68	19
20		Tina Wright	67	20
21		Uma Scott	66	21
22		Victor Green	65	22
23		Wendy Adams	64	23
24		Xavier Nelson	63	24
25		Yolanda Carter	62	25
26		Zachary Perez	61	26
27		Amelia Baker	60	27
28		Benjamin Rivera	59	28

Bersambung ke halaman berikutnya

Tabel II.4 Comprehensive Data Table Example (lanjutan)

ID	Name	Score	Rank
29	Charlotte Rogers	58	29
30	David Murphy	57	30
31	Ethan Cooper	56	31
32	Fiona Reed	55	32
33	George Bailey	54	33
34	Hannah Cox	53	34
35	Isaac Howard	52	35
36	Julia Ward	51	36
37	Kyle Flores	50	37
38	Lily Bell	49	38
39	Mason Sanders	48	39
40	Nora Patterson	47	40
41	Owen Ramirez	46	41
42	Penelope Torres	45	42
43	Quentin Foster	44	43
44	Rebecca Gonzales	43	44
45	Sebastian Bryant	42	45
46	Taylor Alexander	41	46
47	Ursula Russell	40	47
48	Vincent Griffin	39	48
49	William Diaz	38	49
50	Zoe Simmons	37	50

II.4.2.4 Beberapa Contoh Penulisan Rumus atau Persamaan Matematika Menggunakan LaTeX Termasuk Penomorannya

Contoh rumus matematika dapat ditulis seperti pada Persamaan **??** di bawah ini. Penomoran persamaan diletakkan di sebelah kanan, dan rumus ditulis dalam mode *display math*.

$$E = mc^2 \tag{II.1}$$

Contoh lain penulisan rumus matematika yang lebih kompleks dapat ditulis seperti pada Persamaan **??**.

$$f(x) = ax^2 + bx + c \tag{II.2}$$

$$\begin{aligned} f'(x) &= \frac{d}{dx}(ax^2 + bx + c) \\ &= 2ax + b \end{aligned} \tag{II.3}$$

Jika rumus terlalu panjang untuk ditulis dalam satu baris, gunakan lingkungan *multline* seperti pada Persamaan **??** di bawah ini.

$$\begin{aligned} y = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7 \\ + a_8x^8 + a_9x^9 + a_{10}x^{10} \end{aligned} \tag{II.4}$$

Jika ada penurunan rumus yang terdiri dari beberapa baris, namun tidak memerlukan penomoran pada setiap baris, gunakan lingkungan *align**, misalnya:

$$\begin{aligned} S &= \sum_{i=1}^{n} i^2 \\ &= 1^2 + 2^2 + 3^2 + \cdots + n^2 \\ &= \frac{n(n+1)(2n+1)}{6} \end{aligned}$$

Contoh lainnya adalah rumus untuk mencari nilai rata-rata fungsi $f(x)$ pada interval $[p, q]$:

$$\begin{aligned} \bar{f} &= \frac{1}{q-p}\int_p^q f(x)\,dx \\ &= \frac{1}{q-p}\int_p^q (ax^2 + bx + c)\,dx \\ &= \frac{1}{q-p}\left[\frac{a}{3}x^3 + \frac{b}{2}x^2 + cx\right]_p^q \\ &= \frac{a(q^3-p^3)}{3(q-p)} + \frac{b(q^2-p^2)}{2(q-p)} + c \end{aligned}$$

II.4.3 Algoritma, Pseudocode, atau Kode

Contoh penulisan algoritma atau pseudocode dapat ditulis seperti pada Kode **??** di bawah ini. Gunakan paket *listings* untuk menulis source code dalam bahasa pemrograman tertentu, seperti pada Kode **??**.

Tabel II.5 Contoh penggunaan kata ”sedangkan” dan ”sehingga”

Kata	Salah	Benar
sedangkan	Sedangkan sistem lama masih digunakan oleh banyak pengguna.	Sistem lama masih digunakan oleh banyak pengguna, sedangkan sistem baru belum siap.
sehingga	Sehingga sistem lama masih digunakan oleh banyak pengguna.	Sistem lama masih digunakan oleh banyak pengguna sehingga sistem baru belum siap.

Kode II.1 Contoh pseudocode

```
ALGORITHM HelloWorld
   PRINT "Hello, World!"
END ALGORITHM
```

Kode II.2 Contoh source code Python

```
def hello_world():
    print("Hello, World!")
hello_world()
```

II.5 Beberapa Kesalahan Penulisan yang Sering Terjadi

II.5.1 Penggunaan Kata ”di mana” atau ”dimana”

Banyak yang menuliskan kata ”di mana” atau ”dimana” sebagai pengganti kata ”which” dalam bahasa Inggris. Padahal, penggunaan kata ”di mana” atau ”dimana” tidak tepat dalam konteks tersebut. Demikian juga untuk kata serupa, misalnya ”yang mana”. Kata ”di mana” atau ”dimana” ini harus diganti dengan kata lain, seperti ”dengan”, ”tempat”, ”yang”, dan sebagainya tergantung kalimatnya. Penjelasan lengkap dapat dilihat pada (*Buku Praktis Bahasa Indonesia 1/Kata - Wikisumber bahasa Indonesia* 2024).

II.5.2 Penggunaan Kata ”sedangkan” dan ”sehingga”

Kata ”sedangkan” dan ”sehingga” adalah kata hubung atau konjungsi. Konjungsi adalah kata atau ungkapan yang menghubungkan satuan bahasa (kata, frasa, klausa, dan kalimat). Konjungsi dapat dibagi menjadi konjungsi intrakalimat dan antarkalimat. Kata ”sedangkan” menghubungkan dua klausa yang bersifat kontrasif, sedangkan ”sehingga” menghubungkan dua klausa yang bersifat kausal. Dalam ragam formal, kata hubung “sedangkan” dan

“sehingga” hanya dapat digunakan sebagai konjungsi intrakalimat sehingga kedua konjungsi itu **tidak dapat diletakkan pada awal kalimat**. Selain itu, penggunaan kata ”sedangkan” harus didahului oleh koma (,), sedangkan kata ”sehingga” tidak perlu didahului oleh koma (,). Contoh penggunaan yang benar dan salah dapat dilihat pada Tabel **??**.

II.5.3 Penggunaan Istilah yang Tidak Baku

Ada beberapa istilah yang sering digunakan dalam pembicaraan sehari-hari, tetapi tidak baku dalam penulisan ilmiah. Beberapa istilah tersebut antara lain:

(a) analisa → analisis
(b) eksisting atau existing → yang ada atau saat ini
(c) bisnis proses → proses bisnis
(d) user → pengguna
(e) system → sistem
(f) database → basis data
(g) aktifitas → aktivitas
(h) efektifitas → efektivitas
(i) sosial media → media sosial

II.5.4 Pemisah Desimal dan Ribuan

Tanda pemisah desimal dalam bahasa Indonesia adalah tanda koma, contoh:

(a) (Salah) Akurasi naik menjadi 50.6%
(b) (Benar) Akurasi naik menjadi 50,6%

II.5.5 Daftar atau *List*

Ada beberapa aturan penulisan daftar atau *list* yang perlu diperhatikan, antara lain:

a) Jika memungkinkan, hindari penggunaan “bullet points” atau sejenisnya. Sebaiknya, gunakan angka (1, 2, 3, ...) atau huruf (a, b, c, …). Dengan demikian, pembaca dapat dengan mudah melihat jumlah *item* atau *list*.
b) Jika dalam daftar hanya ada satu item, tidak perlu menggunakan nomor urut.
c) Penjelasan atau deskripsi suatu item sebaiknya menyatu dengan judul item tersebut, tidak berbeda halaman. Contoh yang salah: judul item

ada di halaman 10, namun deskripsinya di halaman 11. Sebaiknya pindahkan judul tersebut ke halaman 11.

d) Jika penjelasan atau deskripsi suatu item cukup panjang, misalnya lebih dari 1 halaman atau terdiri atas beberapa paragraf, sebaiknya setiap item tersebut dijadikan judul subbab, kecuali jika level subbab sudah mencapai level 4.

II.5.6 Penggunaan Kata ”masing-masing” dan ”setiap”

Kata “masing-masing” digunakan di belakang kata yang diterangkan, misalnya ”Setiap proses menggunakan algoritma masing-masing”. Kata “tiap-tiap” atau “setiap” ditempatkan di depan kata yang diterangkan, misalnya ”Setiap proses menggunakan algoritma tertentu”.

BAB III
ANALISIS MASALAH

III.1 Analisis Kondisi Saat Ini

Menurut Laudon **and** Laudon (2020), gambarkan terlebih dahulu model konseptual sistem yang ada saat ini. Model konseptual ini berisi berbagai komponen atau subsitem dan interaksi antarsubsistem tersebut. Setelah itu, berikan penjelasan tentang masalah yang ada pada sistem tersebut. Paragraf berikut berisi contoh penjabaran masalah sistem informasi fasilitas kesehatan untuk pasien (Pressman 2019).

III.2 Analisis Kebutuhan

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

III.2.1 Identifikasi Masalah Pengguna

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est.

Curabitur consectetuer.

III.2.2 Kebutuhan Fungsional

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

III.2.3 Kebutuhan Nonfungsional

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

III.3 Analisis Pemilihan Solusi

III.3.1 Alternatif Solusi

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetuer at, consectetuer sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.

III.3.2 Analisis Penentuan Solusi

Morbi luctus, wisi viverra faucibus pretium, nibh est placerat odio, nec commodo wisi enim eget quam. Quisque libero justo, consectetuer a, feugiat vitae, porttitor eu, libero. Suspendisse sed mauris vitae elit sollicitudin malesuada. Maecenas ultricies eros sit amet ante. Ut venenatis velit. Maecenas sed mi eget dui varius euismod. Phasellus aliquet volutpat odio. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque sit amet pede ac sem eleifend consectetuer. Nullam elementum, urna vel imperdiet sodales, elit ipsum pharetra ligula, ac pretium ante justo a nulla. Curabitur tristique arcu eu metus. Vestibulum lectus. Proin mauris. Proin eu nunc eu urna hendrerit faucibus. Aliquam auctor, pede consequat laoreet varius, eros tellus scelerisque quam, pellentesque hendrerit ipsum dolor sed augue. Nulla nec lacus.

BAB IV
DESAIN KONSEP SOLUSI

Ilustrasikan desain konsep solusi dalam bentuk model konseptual dan penjelasan secara ringkas, beserta perbedaannya dengan sistem saat ini. Ilustrasi harus dapat dibandingkan (*before* and *after*). Karena masih berupa proposal, bab ini hanya berisi gambar desain konsep solusi tersebut dan penjelasan perbandingannya dengan gambar sistem yang ada saat ini (yang tergambar di awal Bab **??**).

BAB V
RENCANA SELANJUTNYA

Jelaskan secara detail langkah-langkah rencana selanjutnya, hal-hal yang diperlukan atau akan disiapkan, dan risiko dan mitigasinya, yang meliputi:

(a) Rencana implementasi, termasuk alat dan bahan yang diperlukan, lingkungan, konfigurasi, biaya, dan sebagainya.
(b) Desain pengujian dan evaluasi, misalnya metode verifikasi dan validasi.
(c) Analisis risiko dan mitigasi, misalnya tindakan selanjutnya jika ada yang tidak berjalan sesuai rencana.

DAFTAR PUSTAKA

Buku Praktis Bahasa Indonesia 1/Kata - Wikisumber bahasa Indonesia. 2024. **urlseen** 22 **october** 2025. https://id.wikisource.org/wiki/Buku_Praktis_Bahasa_Indonesia_1/Kata.

Laudon, Kenneth C. **and** Jane P. Laudon. 2020. *Sistem Informasi Manajemen.* Jakarta: Pearson Education.

Pressman, Roger S. 2019. *Rekayasa Perangkat Lunak: Pendekatan Praktisi.* Yogyakarta: McGraw-Hill Education.