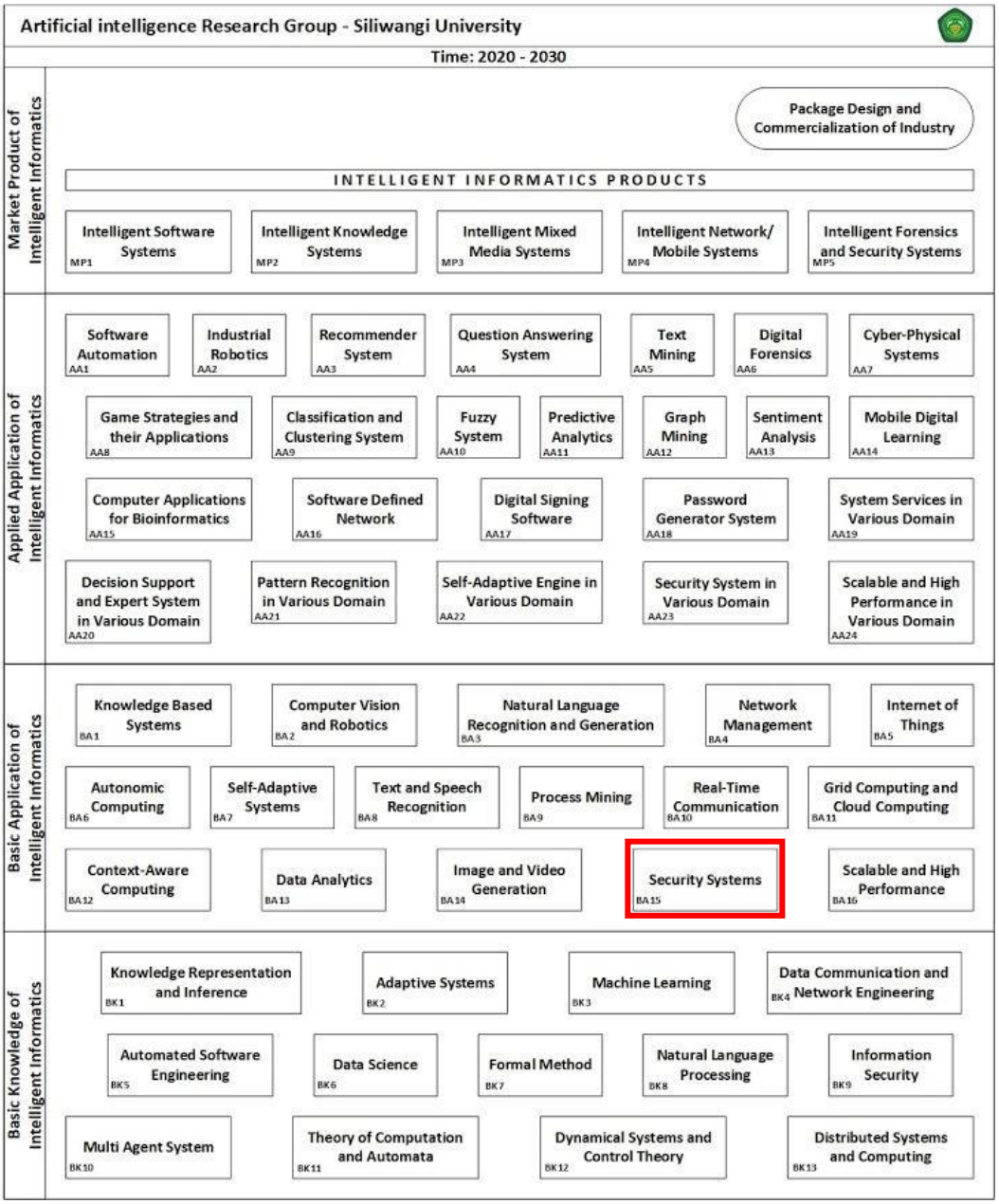
BAB III

METODOLOGI PENELITIAN

3.1 *Road Map* Penelitian

Gambar 3.1 menyajikan *Road Map* pada penelitian ini.

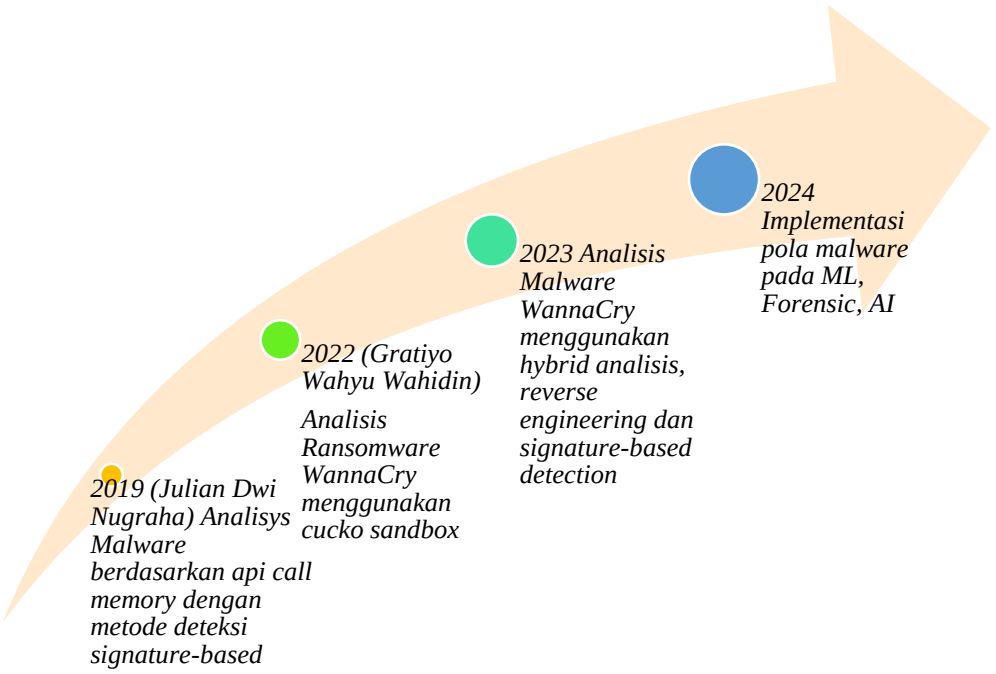


Gambar 3.1 *Road Map* 1

Road Map penelitian dibagi menjadi 4 bagian yaitu :

1. *Market product of intelligent informatics* merupakan *Market Product of Intelligent Informatics* adalah istilah yang mengacu pada produk-produk atau solusi yang dikembangkan dalam bidang informasi cerdas *(intelligent informatics)* dan ditujukan untuk pasar atau konsumen. Informasi cerdas melibatkan penggunaan teknologi seperti kecerdasan buatan (*artificial intelligence)*, analitik data, pembelajaran mesin, dan komputasi cerdas dalam mengolah dan menganalisis data dengan tujuan menghasilkan wawasan, prediksi, atau solusi yang cerdas.
2. *Aplied Application of Intelligent Informatics* merupakan *Application of Intelligent Informatics* (Aplikasi Informasi Cerdas) merujuk pada penerapan teknologi informasi cerdas, seperti kecerdasan buatan *(artificial intelligence)*, analitik data, pembelajaran mesin, dan komputasi cerdas dalam berbagai bidang atau domain tertentu. Aplikasi ini bertujuan mengoptimalkan proses, meningkatkan kinerja, mengambil keputusan yang lebih cerdas, dan memberikan nilai tambah di berbagai sektor.
3. *Basic Aplication of intelligent Informatic* merupakan *Basic Application of Intelligent Informatics* (Aplikasi Dasar Informasi Cerdas) merujuk pada penggunaan teknologi informasi cerdas dalam skala yang lebih sederhana dan mendasar. Ini mencakup penggunaan konsep dan algoritma kecerdasan buatan, analitik data, pembelajaran mesin, dan komputasi cerdas untuk menghasilkan solusi yang lebih sederhana dan mudah diimplementasikan.

4. *Basic Knowledge of Intelligent Informatics* merupakan pengetahuan Dasar tentang Informasi Cerdas merupakan fondasi yang penting untuk memahami dan berpartisipasi dalam pengembangan dan penerapan teknologi informasi cerdas. Hal ini membantu individu memahami konsep-konsep dasar, mempelajari alat dan teknik yang digunakan dalam praktik, serta memahami implikasi dan potensi teknologi informasi cerdas dalam berbagai konteks



Gambar 3.2 *Road Map* Penelitian 2

Road map pada gambar 3.2 penelitian merujuk dari point road map *AIS Security System* pada gambar sebelumnya yang berhubungan dengan *malware* analisis. *Security System* (Sistem Keamanan) seperangkat langkah, proses, perangkat keras, perangkat lunak, dan kebijakan yang dirancang melindungi suatu entitas atau sistem dari ancaman, serangan, atau akses yang tidak sah. Tujuan dari Security *System* adalah menjaga kerahasiaan, integritas, dan keamanan.

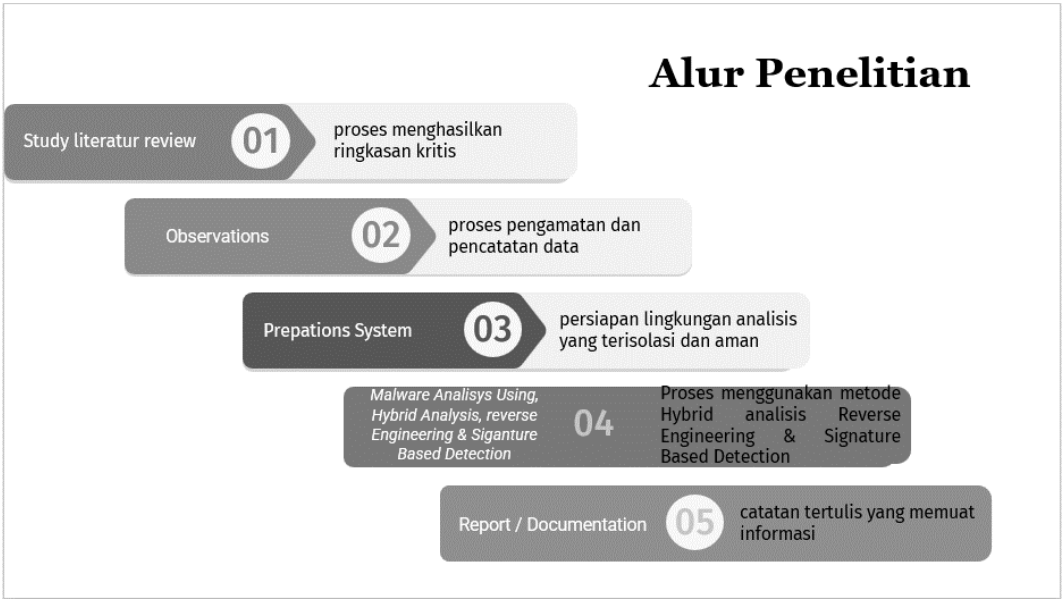
Berdasarkan roadmap gambar 3.2 penelitian ini merancang point – point dalam melihat peluang penelitian selanjutnya, diantaranya

1. 2019 (Julian Dwi Nugraha) Analisis *Malware* berdasarkan *api call memory* dengan metode deteksi *signature-based,* dimana poin utama penelitian ini menghasilkan *signature* yang didapat dari *API CALL Memory.*
2. 2022 (Gratiyo Wahyu Wahidin) *Analysis Ransomware WannaCry* menggunakan *cucko sandbox,* dimana point utamanya adalah data karakter dari *malware* tersebut. Data tersebut berupa informasi yang penting untuk menggali rekam jejak dari apa saja yang dilakukan *malware* pada perangkat lunak yang terinfeksi, seperti halnya pada analisis yang telah dilakukan *malware* melakukan akses dan merubah beberapa komponen penting pada proses komputer.
3. 2023 *Analysis Malware WannaCry* menggunakan *hybrid analysis*, *reverse engineering* dan *signature-based detection, dan*
4. 2024 Implementasi pola *malware pada ML, Forensic, AI.* Peneliti melihat bahwa kombinasi ML, Forensik, dan AI dalam Keamanan *Malware,* seperti :
    a. Integrasi teknik ML dan forensik digital untuk deteksi dan analisis *malware* yang lebih efektif.
    b. Penggunaan AI dalam proses forensik dalam mengotomatisasi analisis dan respon terhadap serangan *malware.*
    c. *Trend* terkini dalam pengembangan solusi keamanan berbasis ML dan AI untuk melawan *malware.*

Materi tersebut dapat dikembangkan lebih lanjut dengan mengeksplorasi studi kasus, implementasi nyata, dan konteks yang lebih mendalam dalam masing-masing topik. Penting untuk menyebutkan bahwa perkembangan dalam keamanan *cyber* terus berlanjut, oleh karena itu, penting untuk mengacu pada literatur terkini dan riset terbaru saat menyusun materi tentang implementasi pola *malware* pada ML, Forensik, dan AI.

3.2 Tahapan Penelitian

Alur penelitian pada gambar 3.3, terdiri dari lima bagian utama, pertama yang ditempuh adalah *Study Literature Review*, dilanjutkan dengan melakukan *observations*, lalu *proses prepations systems*, setelah itu melakukan *malware analysis using hybrid analisys, reverse engineering and signature-based detection* dan diakhiri dengan *report* atau *documentation.*



Gambar 3.3 Alur Penelitian

Penjelasan mengenai alur penelitian dapat diuraikan sebagai berikut:

a. *Study Literature Review*

Study Literature yang dipakai merupakan literatur yang relevan dengan topik yang akan diteliti. Sumber literatur yang dapat dicari antara lain jurnal ilmiah, paper, dan artikel dari situs-situs terpercaya seperti situs resmi organisasi keamanan *cyber* atau situs berita terkait keamanan *cyber* selain itu mempelajari konsep dasar teknik *reverse engineering* dan *signature-based detection.*

b. *Observations*

Observations yang dilakukan adalah mengumpulkan sampel *malware WannaCry* untuk penelitian. Sampel *malware* dapat diperoleh dari sumber yang dapat dipercaya dan aman, disini saya mengambil dari website *https:any.run.*

c. *Prepations*

Prepations system analisis *malware WannaCry* menggunakan teknik *reverse engineering* dan *signature-based detection*. Selain itu, harus memiliki pengetahuan tentang perilaku *malware*, karakteristik *malware*, sistem operasi, pemrograman, jaringan, dan keamanan informasi. Diperlukan juga untuk melakukan analisis *malware WannaCry adalah decompiler, disassembler, debugger,* dan analisis *malware tools* seperti IDA Pro, PeStudio, Ghidra, *Hash*Call, PeStudio,*Process* Monitor dan ApateDNS..

d. *Malware Analysis Using Hybrid Analysis, Reverse Engineering and Signature-based Detection.*

Proses analisis dikhususkan pada *signature malware WannaCry*, dengan tujuan penelitian pola *byte* dan kode instruksi tertentu, diawali dengan *analysis hybrid*

untuk menghasilkan *reverse engineering* dan *signature-based detection* ditunjukkan dengan beberapa sample yang nantinya dicocokkan antara dua metode yang digunakan.

e. *Report / Documentation*

Report / Documentation pada analisis *malware WannaCry* dengan metode *reverse engineering* dan *signature-based detection* dapat dilakukan membuat laporan atau dokumen, foto serta video yang berisi informasi tentang *malware WannaCry,* teknik *reverse engineering* dan *signature-based detection* yang digunakan dalam analisis, dan hasil dari analisis tersebut, seperti di sisipkan hasil berupa foto atau vidio dalam investigasi *malware WannaCry* analisis, serta menjelaskan karakteristik dan struktur dari *malware WannaCry,* pola *byte,* kode instruksi serta cara kerja dan dampaknya pada sistem yang terinfeksi.