BAB III
METODOLOGI PENELITIAN

3.1 Metodologi Penelitian

Metode penelitian adalah tata cara terstruktur yang digunakan dalam memperoleh data berupa informasi dan ditujukan untuk memecahkan permasalahan yang ditemukan pada perancangan.

3.2 Jenis Pendekatan

Jenis Pendekatan adalah teknis yang digunakan untuk menganalisis data yang diperlukan untuk meneliti topik perancangan. Maka dari itu, perancangan ini akan menggunakan metode peniltian kualitatif. Penilitian kualitatif merupakan metode yang digunakan untuk memahami topik perancangan secara lebih dalam serta memperoleh data berupa infromasi yang bersifat aktual [28].

Pada perancangan ini, objek utama yang akan diteliti oleh perancang adalah *cryptojacking*. Penelitian ini akan berfokus untuk mendalami karakteristik dari *cryptojacking* hingga membentuk suatu kesimpulan mengenai bagaimana tindakan preventif yang dapat dilakukan oleh khalayak awam yang nantinya akan dibentuk ke dalam media *motion graphics*.

3.3 Objek dan Subjek Penelitian

3.3.1 Objek Penelitian

Objek penelitian merupakan titik fokus utama yang telah ditetapkan sebagai sumber untuk mendapatkan data yang dibutuhkan. Pada perancangan ini, *cryptojacking* dipilih sebagai objek utama yang diteleti. Maka dari itu, pengumupulan data akan menggunakan data-data yang berupa *report* atau laporan tahunan yang diperoleh dari perusahaan yang berorientasi dalam bidang keamanan siber seperti seperti Cisco, Kaprseky, Symantec, hingga Interpol.

3.3.2 Subjek Penelitian

Subjek penelitan adalah individu yang dinilai kredibel sebagai salah satu sumber untuk memperoleh data yang diperlukan dalam melakukan penelitian. Pemilihan individu dinilai dari adanya keterkaitan antara pengalaman individu dengan topik perancangan. Subjek penelitian yang digunakan pada perancangan ini adalah Bapak Wahyu Adi Prabowo, S. Kom., M.B.A., M. Kom. yang berprofesi sebagai dosen di IT Telkom Purwokerto yang telah tersertifikasi secara Internasional sebagai ethical hacker yang bertugas pada maintenance system di Red Hat, Black Hat, dan Grey Hat.

3.4 Jenis dan Sumber Data

3.4.1 Sumber Primer

Sumber data primer merupakan informasi yang didapatkan secara langsung oleh perancang. Dalam perancangan ini, sumber informasi primer didapatkan dari hasil wawancara dengan narasumber Bapak Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom. dosen dari IT Telkom Purwokerto dan *certified ethical hacker* dari Red Hat. Adapun jenis data yang diterima yakni jawaban atas pertanyaan yang telah ditanyakan oleh perancang.

3.4.2 Sumber Sekunder

Sumber data sakunder merupakan data yang tidak diperoleh secara langsung oleh perancang. Maka, pengumpulan data dengan menggunakan sumber sakunder biasanya menggunakan bantuan yang dapat berupa buku, dokumen, internet, dan studi literatur. Jenis data yang didapatkan nantinya akan berupa seperti grafik, diagaram dan gambar.

3.5 Teknik Pengeumpulan Data

3.5.1 Wawancara

Metode wawancara yang digunakan pada perancangan ini adalah metode wawancara tidak tersteruktur. Metode wawancara tidak terstruktur digunakan untuk memperdalam dan memperkuat data yang telah ditemukan [28]. Dalam perancangan ini, topik yang akan ditanyakan adalah mengenai keamanan siber secara umum yang kemudian nantinya akan dikhususkan kedalam *cryptojacking*.

3.5.2 Observasi

Menurut Sutrisno Hadi yang dilansir dari buku Metode Penelitian Kuatitatif, Kualitatif dan R&D, observasi merupakan sebuah tindakan melakukan pengamatan pada suatu objek yang telah ditetapkan dalam sebuah penelitian [28]. Observasi ditujukan untuk mempelajari lebih detail mengenai objek yang sedang diteleti untuk mendapatkan informasi yang nantinya akan digunakan sebagai salah satu sumber data.

Pada perancangan ini, obeservasi dilakukan dengan mengamati berita-berita yang berhubungan dengan *cryptojacking* yang ditemukan oleh perancang dalam ranah Internet.

3.5.3 Studi Literatur

Studi literatur adalah sebuah penelitian yang digunakan untuk memahami lebih dalam mengenai suatu gejela, fenomena maupun objek yang sedang diteliti. Penelitian yang dilakukan dengan studi literatur menggunakan sumber imliah yang telah ada sebelumnya seperti buku, ensiklopedi, hingga laporan ilmiah.

Pada perancangan ini, studi literatur digunakan untuk memperoleh data-data yang berhubungan dengan *cryptojacking*. Data-data tersebut dapat berbentuk seperti infromasi perkembangan kasus, bagaimana cara

mengindetifikasi kasus tersebut, hingga tindakan preventif yang dapat digunakan oleh khalayak yang masih awam.

3.6 Metode Analisis Data

Metode analisis data yang digunakan dalam penelitian ini adalah SWOT. SWOT merupakan sebuah analisis yang menggunakan beberapa jenis analisis didalamnya seperti Kekuatan (*Strenghts*), Kelemahan (*Weakness*), Peluang (*Opportunity*), dan Ancaman (*Threat*).

Tujuan dari dilakukannya analisis ini adalah untuk menentukan USP atau *Unique Selling Point* yakni kelebihan yang dapat ditemukan pada karya yang akan dirancang. Kemudian, hasil dari analisis SWOT juga dapat digunakan untuk menentukan posisi atau positioning dari perancangan ini nantinya dalam perancangan yang telah dilakukan sebelumnya.

3.7 Identifikasi Data

Identifikasi data ditujukan untuk meninjau kembali data yang telah ditemukan menggunakan metode penelitian yang telah dipilih. Peninjauan data digunakan oleh merumuskan kesimpulan dari penelitan yang telah dilakukan.

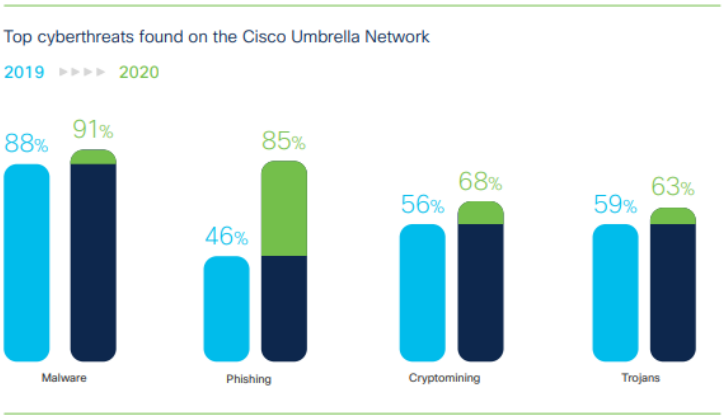
3.7.1 Profil Instansi

Nama Instansi	: PT. Cisco System Indonesia
Alamat Instansi	: Jl. Gatot Subroto No.kav 18, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12710
Telepon	: (021)-27546400

Gambar 3.1 Logo Cisco System, Inc.
Sumber: cisco.com/logo

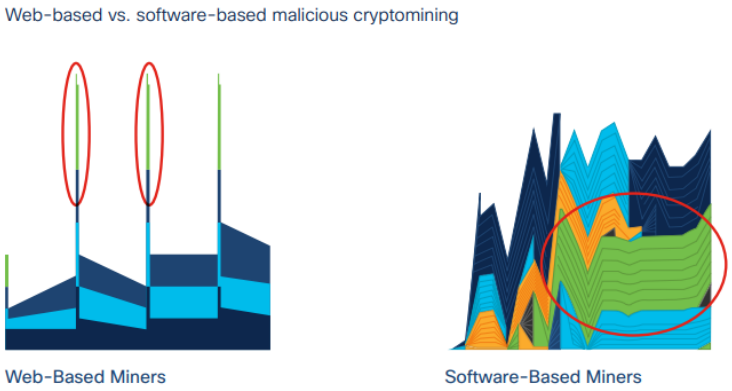
Cisco merupakan sebuah perusahan yang menawarkan berbagai solusi yang berhubungan dengan teknologi hingga menjadi salah satu penyedia layanan keamanan siber. Cisco didirikan pada tahun 1984 oleh beberapa saintis yang berasal dari Standford University. Pada penelitian ini, Cisco merupakan salah satu sumber data utama yang meyediakan berbagai data mengenai *cryptojacking* yang dilengkap informasi berupa grafik, diagram, hingga gambar.

Berdasarkan data yang ditemukan dari report yang dirlis oleh cisco umbrella pada November 2020, ditemukan adanya empat jenis ancaman yang yang paling banyak digunakan dalam melakukan kejahatan siber. Salah satu ancaman tersebut adalah cryptomining atau dikenal juga dengan istilah *cryptojacking*. *Cryptojacking* merupakan sebuah bentuk serangan siber yang dilakukan untuk menggunakan daya komputasi perangkat elektronik orang lain seperti laptop, computer, hingga smartphone untuk memproduksi mata uang digital.



Gambar 3.2 Grafik peningkatan serangan siber pada Cicso Umbrella Network
Sumber: Report the modern cybersecurity landscape: scaling for motion

Pada grafik diatas dapat dilihat adanya peningkatan antara aktivitas serangan siber khsuusnya dalam hal ini cryptomining dari tahun 2019 ke tahun 2020 sebanyak 12%. Peningktan aktivitas dari *cryptojacking* dapat terus bertambah seiiring dengan perkembangan penggunaan mata uang digital yang semakin umum untuk digunakan.



Gambar 3.3 Perbandingan antara virus *cryptojacking* yang berjalan pada web dan perangkat lunak.
Sumber: Report the modern cybersecurity landscape: scaling for motion

Serangan siber menggunakan virus *cryptojacking* biasanya dapat ditemukan dalam dua jenis yakni *cryptojacking* yang berjalan pada web

browser dan yang terintegrasi langusng dengan komputer dengan menggunakan software yang sudah terinstall tanpa sepengetahuan dari pemilik perangkat tersebut. Perbedaan yang terdapat diantara keduanya terletak pada tempat dari virus tersebut dibenamkan. Virus *cryptojacking* yang dimuat dalam sebuah website biasnaya akan mulai bekerja ketika kita mengakses website tersebut sedangkan virus *cryptojacking* yang berjalan pada perangkat lunak dapat menyebabkan kerusakan yang lebih serius pada perangkat komputer itu sendiri.

Gambar 3.4 Serangan siber tertinggi pada Cisco Umbrella Network
Sumber: Report the modern cybersecurity landscape: scaling for motion

Sistem dari Cisco Umbrella Network menemukan bahwasnaya *cryptojacking* menempati urutan pertama sebagai salah satu jenis serangan siber yang paling dominan dari tahun 2019 sampai dengan tahun 2020. Adapun penyabab dari naiknya kasus *cryptojacking* tersebut diletarbelakangi oleh beberapa aspek seperti, mudahnya para pelaku kejatan siber dalam mendapatkan keuntungan berbentuk mata uang digital yang dapat digunakan sebagai alat transaksi. Virus *cryptojacking* yang masih terkesan sulit untuk dideteksi sedini mungkin hingga masih adanya anggapan khayalak bahwa virus dari *cryptojacking* itu sendiri tidak berbahaya jika dibandingkan dengan serangan siber lainnya. Namun, pada kenyataan virus dari *cryptojacking* dapat

menimbulkan kurugian yang cukup besar dikarenakan mempunyai pengaruh langsung terhadap kesehatan dari suatu perangkat elektronik serta berpotensi menimbulkan berbagai kerugian lainnya.

3.7.2 Observasi

Dalam perancangan ini, observasi dilakukan secara dengan mengamati berita mengenai kasus-kasus yang berhubungan dengan *cryptojacking* ini. Dari pengamantan yang dilakukan ditremukan masih banyaknya kasus yang berkaitain dengan potensi dari crypotjacking ini. Seperti yang dilansir dari beberapa media nasional seperti CNN yang melansir bahwasanya adanya potensi antara ponsel dan laptop yang semakin lemot dapat diakibatkan oleh *cryptojacking* [29]. Hal tersebut terjadi dikarena perankgat yang sudah terinfeksi oleh cryptojacknig dipaksa untuk bekerja sekeras mungkin sehingga memakai lebih banyak sumber daya yang terdapat pada perangakt tersebut. Kemudian dilansir dari The International Criminal Police Organization (Interpol) *Cryptojacking* dapat menginfeksi sebuah perangkat dapat melalui beberapa metode [12]. Metode yang dapat digunakan seperti mengakses pranala yang terlampir pada e-mail yang dikirim oleh orang yang tidak diketahui hingga mengunjungi website yang telah dinfeksi oleh *cryptojacking* itu sendiri.

3.7.3 Wawancara

Gambar 3.5 Wawancara dengan narasumber
Sumber: Data pribadi

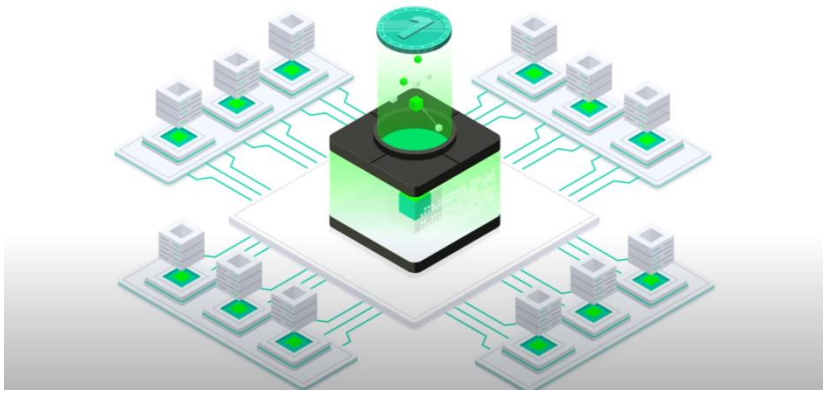
Pada perancangan ini wawancara dilakukan dengan Bapak Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom. yang berprofesi sebagai salah satu dosen yang mengajar di Institut Teknologi Telkom Purwokerto dan juga berprofesi sebagai Ethical Hacker yang telah tersertifikasi Red Hat, Black Hat dan Grey Hat yang bertugas dalam maintenance system.

Beliau menjelaskan, *cryptojacking* merupakan salah satu jenis serangan siber yang cukup unik dikarenakan sulitnya deteksi yang dapat dilakukan oleh individu yang kurang memahami akan *cryptojacking* itu sendiri. Adapun hal yang paling mencolok dari infeksi yang dilakukan *cryptojacking* itu sendiri dapat ditemukan pada adanya penurunan performa yang cukup siginifikan terhadap daya komputasi pada perangkat yang telah terinfeksi. Beliau juga menambahkan, perkembangan *cryptojacking* juga diikuti berkat penggunaan mata uang digital seperti *cryptocurrency* yang mulai digunakan sebagai alat pembayaran untuk kebutuhan sehari-hari.

Adapun kesimpulan yang saya dapatkan dari wawancara yang saya lakukan adalah untuk mengubah target audiens secara lebih spesifik. Maka dari itu perancangan ini akan berfokus kepada upaya edukasi masyarakat yang masih awam mengenai pengenalan dan bagaimana tindakan preventif yang dapat dilakukan. Dalam melakukan sebuah edukasi maka dibutuhkan sumber data yang kredibel untuk menyampaikan sebuah informasi yang akurat. Maka dari itu, penggunaan data dan informasi yang digunakan dalam perancangan ini akan menggunakan data yang diperoleh dari perusahaan maupun lembaga yang sudah bersifat internasional. Hal tersebut berbanding lurus dengan penjelasan beliau mengenai penggunan sumber data yang digunakan dari perusahaan maupun organanisasi yang sudah bersifat internasional seperti Cisco, IBM, Kaprseky, Australian Cyber Security Center sudah dinilai layak dan kredibel. Beliau menjelaskan penggunaan sumber data yang telah digunakan secara internasional sudah menjadi standar yang wajib untuk diterpakan.

3.7.4 Studi Komparasi

a. Video yang berjudul What is *Cryptojacking*? Signs of *Cryptojacking* and How to remove a *Cryptojacking* Script



Gambar 3. 6 Cuplikan layar dari video what is *cryptojacking*?
signs of *cryptojacking* and how to remove a *cryptojacking* script.
Sumber: youtu.be/Nez-niwd63Y

Video ini dirilis oleh Kaspersky pada kanal Youtube mereka pada April 2022. Video ini menjelaskan akan apa itu *cryptojacking*, bagaimana teknis penyebarannya serta bagaimana cara untuk menangani virus *cryptojacking* tersebut. Topik *cryptojacking* yang diangkat dijelaskan dengan menggunakan *motion graphics* dalam bentuk minimalis dengan kombinasi gaya visual flat design dengan perspektif *isometric*.

Video ini dipilih sebagai salah satu studi komparasi dikarenakan adanya persamaan topik, tujuan, serta kualitas video dan kredibilitas informasi yang disampaikan. Persamaan topik dan tujuan yang digunakan dengan perancangan yang akan dilakukan terdapat pada topik yang diangkat yakni *cryptojacking* dan ditujukan untuk melakukan edukasi mengenai bagaimana tindakan preventif yang dapat dilakukan. Kemudian, kualitas dari video yang diproduksi juga dinilai masih layak untuk dinikmati dan terkesan sebagai salah satu konten yang baru diunggah sehingga memiliki keterbaruan data didalamnya.

Adapun perbedaan yang terdapat antara karya ini dengan karya yang akan dirancang terdapat pada gaya bahasa yang digunakan dan teknis kombinasi *motion graphics* yang akan diterapkan. Karya ini menggunakan bahasa inggris sebagai media dalam penyaluran informasi sedangkan pada karya yang akan dirancang menggunakan bahasa Indonesia. Secara teknis pada karya ini menggunakan kombinasi *motion graphics* antara *flat design* dan dengan perspektif *isometric* yang jika dibandingkan dengan karya yang dirancang akan menggunakan kombinasi *motion graphics* antara animasi dua dimensi dan simulasi tiga dimensi. Kemudian, pada konten ini solusi yang diberikan lebih berfokus kepada menawarkan produk atau layanan yang disediakan oleh Kapresky. Maka dari itu, pada perancangan yang akan dilakukan nantinya akan berfokus kepada bagaimana tindakan preventif yang dapat dilakukan tanpa menyematkan layanan sebuah perusahaan tertentu.

b. Video yang berjudul How Can a Computer Be Protected from *Cryptojacking* Programs

Gambar 3.7 Cuplilkan gambar dari video how can a computer be protected from *cryptojacking* programs.
Sumber: youtu.be/PI9zhP8ZvF0

Video ini dirilis oleh Huawei Network pada Oktober 2022 melalui kanal Youtube yang ditujukan untuk media edukasi dalam topik *cryptojacking* serta juga menempatkan iklan produk dan layanan mereka didalamnya.

Video ini digunakan sebagai salah satu studi komprasi dikarenakan masih memiliki kesamaan topik serta media edukasi yang digunakan dengan karya yang akan dirancang. Topik yang dibahas dalam video ini adalah *cryptojacking* dan ditujukan untuk tujuan edukasi. Kemudian, video ini juga memiliki kualitas yang cukup memadai untuk dijadikan sebagai salah satu studi komparasi yang dinilai layak.

Perbedaan yang terdapat pada karya ini dengan karya yang akan dirancang terdapat pada beberapa aspek seperti bahasa yang digunakan, gaya visual, serta konsep video edukasi yang digunakan. Dari segi bahasa, bahasa yang digunakan dalam perancangan ini menggunakan bahasa inggris, sedangkan dalam perancangan yang akan dilakukan menggunakan bahasa Indonesia. Gaya visual yang diterapkan juga

memiliki perbedaan yang cukup signifikan dimana pada peranacangan ini hanya menggunakan *motion graphics* dengan gaya visual illustrasi sederhana. Pada perancangan yang akan dilakukan, gaya visual yang diterapkan menggunaan kombinasi gaya visual dua dan simulasi tiga dimensi yang diberikan dianimasikan secara dinamis. Konsep video edukasi yang digunakan juga berbeda dimana pada karya ini menempatkan adanya iklan sebuah produk atau layanan yang berhubungan dengan keamanan jaringan dimana pada karya yang akan dirancang hanya akan menerapkan edukasi tanpa adanya sebuah iklan didalamnya.

3.7.5 Analisis SWOT

Tabel 3. 1 Analisis SWOT
Sumber: Data pribadi

	Karya Perancang	**What is *Cryptojacking*? Signs of *Cryptojacking* and How to Remove a *Cryptojacking* Script**	**How Can a Computer Be Protected from *Cryptojacking* Programs**
S	Penggunaan kombinasi diseusikan dengan tren masa kini seperti gaya visual 2D & 3D.	Perusahaan telah mempunyai branding yang kuat.	Perusahaan telah mempunyai branding yang kuat.

W	Tahap perancangan pembuatan *motion graphics* yang memerlukan waktu yang cukup lama untuk diproduksi.	Menggunakan gaya animasi dua dimensi yang terlalu formal sehingga penyampaian informasi terkesan kaku.	Hanya menggunakan ilustrasi seadanya.
O	Masih minimnya konten yang membahas megnenai tindakan preventif mengenai *cryptojacking* dengan menggunakan *motion graphics*.	Menjadi salah satu penyedia konten edukasi mengenai *cryptojacking*.	Masih minimnya edukasi mengenai *cryptojacking*.
T	Sistem algoritma seperti Youtube memproitaskan konten “berbayar” pada bagian atas sehingga konten yang akan diproduksi nantinya sulit untuk ditemukan.	Masih sulitnya mengidentifikasi virus *cryptojacking*.	Keyword yang kurang efektif sehingga video ini cukup sulit untuk ditemukan.

3.7.6 USP

USP merupakan keunggalan yang terdapat dalam produk atau jasa yang terdapat sebagai nilai jual baru utama. Keunggulan yang terdapat dalam perancangan ini terdapat pada kombinasi teknis animasi yang diguakan dalam penyampain informasi yang belum pernah diterapkan sebelumnya. Adapun

tujuan penggunaan kombinasi antara animasi dua dimensi dengan animasi tiga dimensi ditujukan untuk membentuk suatu video edukasi yang bukan hanya dapat memberikan informasi namun juga dapat dinikmati. Kemudian, edukasi mengenai *cryptojacking* ini akan menggunakan *motion graphics* dalam Bahasa Indonesia dan dengan fokus utama dalam menyampaikan informasi tanpa menyematkan sebuah layanan atau produk dari perusahaan tertentu.

3.7.7 Positioning

Perancangan *motion graphics* sebagai sarana edukasi bahaya *cryptojacking* hadir sebagai salah satu konten yang dapat menjadi referensi khalayak dalam memahami salah satu jenis serangan siber yang cukup populer pada masa kini yakni *cryptojacking*. Karya ini ditempatkan sebagai salah satu edukasi yang hadir dalam bahasa Indonesia dengan menggunakan gaya visual yang lebih ekspresif dalam penyampaian informasi dengan gaya visualnya. Karya dirancang dengan tidak menggunakan adanya iklan ataupun teknik preventif yang bersifat terlalu teknis dan kompleks sehingga dapat diterima oleh khalayak awam.

3.7.8 Target Audiens

a. Segmentasi

1) Tertarik dengan perkembangan teknologi
2) Mempunyai perangkat elektronik seperti *smartphone* atau laptop dan sejenisnya.
3) Mengikuti perkembangan *cryptocurrency*

b. Targeting

1) Umur: 15=30 tahun
2) Pendidikan: SMA sampai dengan Perguruan tinggi

3.7.9 Target Market

a. Geografis

Mencakup kota-kota besar Indonesia dikarenakan sebagian besar pengguna *cryptocurrency* dan akses informasi yang memadai berada dalam ruang lingkup perkotaan besar.

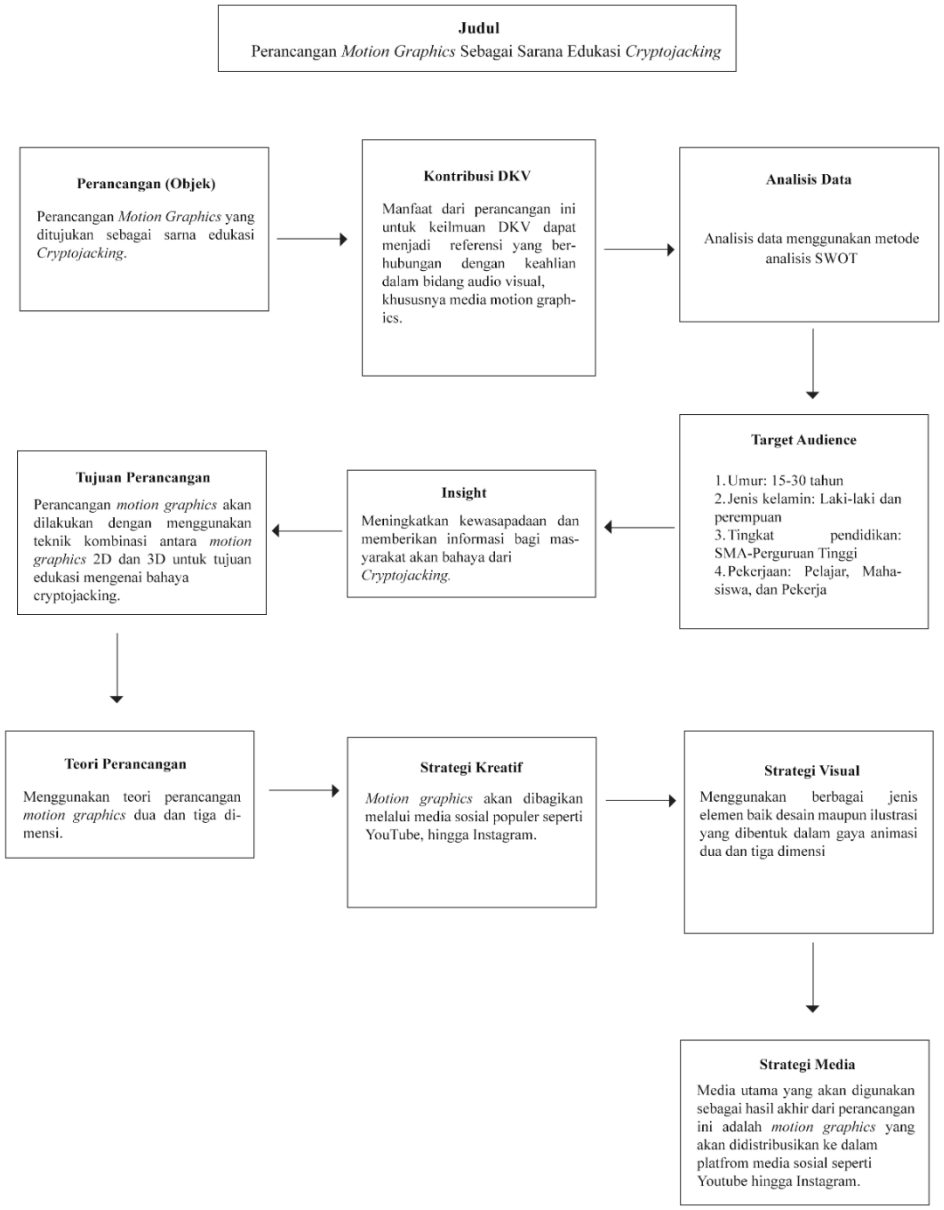
b. Demografis

1) Mengikuti perkembangan teknologi
2) Aktif dalam menggunakan internet dan sosial media
3) Mempunyai *cryptocurrency*
4) Mengikuti perkembangan *cryptocurreny*

c. Psikografis

1) Mengikuti perkembangan teknologi
2) Aktif dalam menggunakan internet dan sosial media
3) Mempunyai *cryptocurrency*
4) Mengikuti perkembangan *cryptocurrency*

3.8 Kerangka Penelitian



Gambar 3.8 Kerangka Penelitian
Sumber: Data pribadi