



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk mengubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

BAB III

METODOLOGI PENELITIAN

3.1 Metode Pengumpulan Data

Penulis menggunakan metodologi hybrid, dimana pengumpulan data dilakukan dengan metode kualitatif dan kuantitatif. Penulis akan melakukan metode kualitatif berupa studi referensi, dengan melakukan pengamatan terhadap sebuah karya visual untuk dijadikan acuan perancangan, serta wawancara kepada ahli digital forensik untuk memperdalam pengetahuan mengenai malware, seperti pencegahan dan penanganannya. Sedangkan untuk metode kuantitatif, penulis akan melakukan survey berupa kuesioner online, untuk mengetahui seberapa dalam pengetahuan masyarakat mengenai malware.

3.1.1 Wawancara

Wawancara dilakukan terhadap Yaman Khaeruzzaman, M.Sc., yang merupakan seorang akademisi, salah satu dosen pengajar di Universitas Multimedia Nusantara, untuk memperdalam informasi seputar malware, mulai dari jenisnya, cara masuknya, pencegahannya, hingga bagaimana mengatasinya. Wawancara dilakukan pada tanggal 14 September 2021 melalui aplikasi Zoom.



Gambar 3.1. Wawancara dengan Yaman Khaeruzzaman, M.Sc.

Yaman menjelaskan bahwa *malware* adalah semua jenis program atau aplikasi yang dengan sengaja menimbulkan kerusakan, baik melalui

server, jaringan, dan lain sebagainya. Yaman juga menjelaskan tidak ada ketetapan jenis *malware* secara umum, jenis *malware* hanya sebagai istilah untuk membedakan setiap karakteristiknya. Misalnya, *virus* merupakan istilah untuk *malware* yang dapat mereplikasi dan masuk kedalam program lain, atau *worm*, *worm* merupakan istilah dari *malware* yang berdiri sendiri dan dapat menduplikasi melalui jaringan, dapat menyebar dari satu perangkat ke perangkat lainnya.

Yaman juga menjelaskan bahwa saat ini, *malware* jenis *Trojan* merupakan yang paling banyak menyerang sebuah perangkat. Untuk mengetahuinya, ada sebuah situs bernama 'honeynet.bssn.co.id', situs tersebut memperlihatkan perkembangan *malware* secara langsung, termasuk informasi bahwa Indonesia menjadi negara dengan kasus serangan *malware* paling tinggi di dunia.

Menurut Yaman, ada beberapa tindakan mendasar untuk melakukan pencegahan *malware* agar tidak masuk kepada perangkat. Yang pertama, dengan menggunakan program *antivirus*. Selain menggunakannya, pengguna juga harus selalu memperbaruinya secara rutin, karena evolusi *malware* bisa saja lebih cepat daripada perkembangan *antivirus* itu sendiri. Selain itu, pengguna juga harus lebih teliti saat melakukan aktivitas daring, seperti tidak membuka sembarangan situs, tidak mengunduh sembarangan file di internet, dan lain sebagainya.

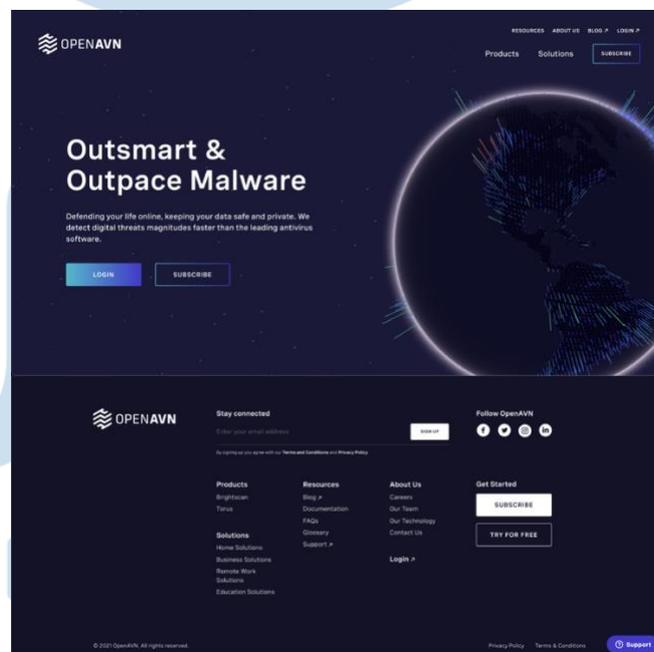
Kesimpulannya, *malware* merupakan program yang sangat sulit dideteksi oleh masyarakat pada umumnya, butuh penggunaan program tertentu untuk bantu mendeteksi, mencegah, dan menghapus *malware* yang ada pada sebuah perangkat. Dengan upaya pencegahan yang telah dilakukan, tidak menutup kemungkinan *malware* akan tetap masuk ke dalam perangkat selagi pengguna terus beraktivitas dengan perangkat yang digunakan, terlebih lagi jika aktivitas tersebut dilakukan secara daring. Oleh karena itu, edukasi mengenai *malware* sangat diperlukan, terutama bagi masyarakat Indonesia yang kesehariannya tidak terlepas dari penggunaan komputer, gawai, laptop, ataupun sejenisnya.

3.1.2 Studi Referensi

Pada metode observasi referensi, penulis mengumpulkan beberapa karya visual untuk dijadikan sebuah acuan dalam visualisasi perancangan media edukasi. Observasi referensi juga digunakan untuk menuntun penulis untuk menciptakan kesatuan pada setiap media yang dirancang. Referensi yang dipilih penulis untuk dijadikan acuan adalah *story telling* yang dibangun pada website Unilever dan penggunaan elemen desain pada website Siemens.

3.1.2.1 Website Open AVN

Open AVN merupakan salah satu karya desain *website* dari sebuah situs yang mengumpulkan perancangan desain *website* bernama Awwwards. Open AVN membahas hal yang serupa dengan topik perancangan yang penulis sedang kerjakan, yaitu *malware*. Akan tetapi, *website* Open AVN lebih cenderung mempromosikan produk anti-virus untuk membasmi *malware*.



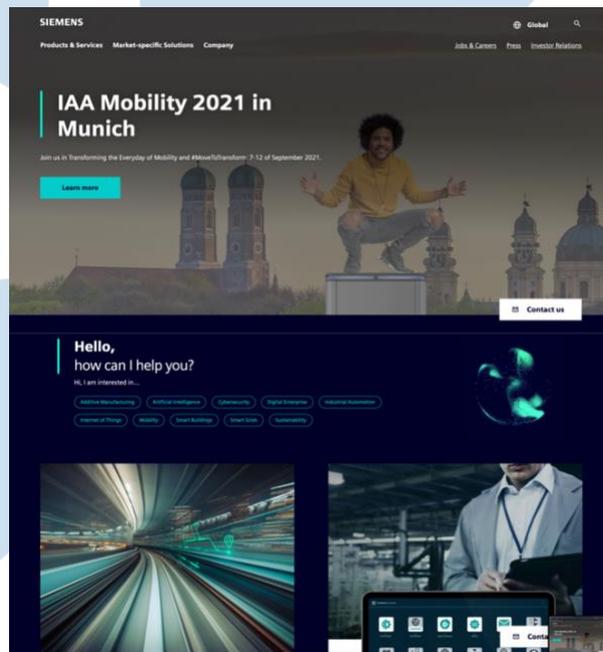
Gambar 3.2. Tampilan Website OPENAVN

Dari segi desain, *website* Open AVN memiliki warna latar belakang yang gelap, dengan elemen visual utama berupa objek tiga

dimensi. Jenis *typefaces* yang digunakan adalah Sans Serif dengan menggunakan warna cerah (putih) untuk memunculkan *contrast* dengan warna latar belakang. Layout yang digunakan juga membuat *readability* dari setiap konten informasi yang diberikan memiliki *hierarchy* yang cukup jelas. Penggunaan elemen visual dan warna yang digunakan memberikan kesan teknologi dan modern. penulis akan mengadopsi beberapa elemen visual.

3.1.2.2 Website Siemens

Siemens merupakan sebuah perusahaan asal Jerman, yang bergerak pada bidang teknologi, industri, infrastruktur, dan perawatan kesehatan. Produk Siemens berupa gawai, mesin dinamo, dan alat-alat kesehatan untuk rumah sakit. Siemens memperkenalkan produknya melalui beragam media, salah satunya adalah *website*.



Gambar 3.3. Tampilan Website Siemens

Melalui website, Siemens memperkenalkan perusahaan serta beragam produk dan jasa yang ditawarkan. Website Siemens menggunakan latar belakang dengan warna yang gelap, menggunakan jenis huruf yang mudah dibaca, dan cenderung

menggunakan foto sebagai visual utamanya. Perpaduan latar belakang yang gelap, pilihan foto yang digunakan, jenis dan warna huruf yang dipakai memberikan kesan teknologi dan futuristis.

3.1.2.3 Kesimpulan Studi Referensi

Berdasarkan kedua referensi yang telah dibahas sebelumnya, penulis akan merancang media edukasi dengan menggunakan *layout* dengan peletakan elemen visual yang sama dengan *website* Open AVN guna mengoptimalkan *readability* konten informasi yang dibagikan. Kemudian pemilihan warna dan huruf yang sejenis dengan *website* Siemens, yaitu huruf yang terkesan kaku dengan keterbacaan yang baik, serta perpaduan warna latar belakang yang gelap dengan warna huruf atau elemen visual yang kontras untuk memberikan kesan teknologi dan futuristis, agar sesuai dengan topik pembahasan informasi yang disampaikan.

3.1.3 Kuesioner

Kuesioner ditujukan kepada masyarakat dengan usia 25-34 tahun di daerah Jawa Barat, DKI Jakarta, dan Jawa Tengah. Tujuan penulis melakukan kuesioner adalah untuk mengetahui aktivitas daring apa saja yang seringkali dilakukan masyarakat, seberapa dalam pengetahuan masyarakat mengenai permasalahan serangan malware, informasi apa saja yang masyarakat butuhkan mengenai *malware*, dan media apa saja yang sekiranya efektif digunakan sebagai perantara untuk menyampaikan informasi kepada masyarakat, khususnya target responden. Kuesioner dilakukan dengan metode *random sampling*, dengan penentuan jumlah sampel menggunakan rumus Slovin dengan derajat ketelitian 10%. Pada tahun 2020, penetrasi pengguna internet di daerah Jawa Barat mencapai 35.100.611 jiwa, Jawa Tengah 26.536.320 jiwa, dan DKI Jakarta 8.928.485 jiwa. Hasil perhitungan memperlihatkan butuh 100 responden untuk memenuhi syarat kuesioner.

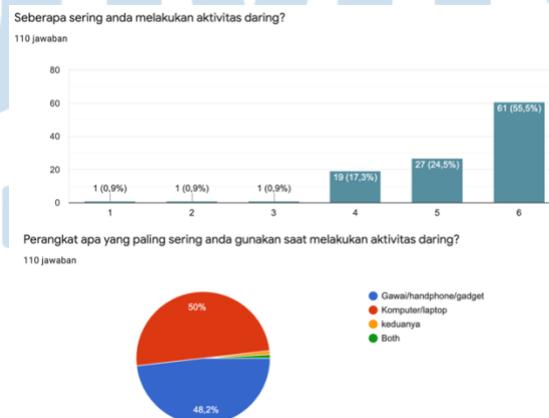
$$n = N (1 + Ne^2)$$

$$\begin{aligned}
 N &= \text{Jumlah Populasi} \\
 &= 35.100.611 + 26.536.320 + 8.928.485 \\
 &= 70.565.416 \\
 e &= \text{Derajat Ketelitian} \\
 &= 10\% \\
 n &= 70.565.416 / (1 + 70.565.416 \times 10\%^2) \\
 &= 70.565.416 / (1 + 70.565.416 \times 0,01) \\
 &= 70.565.416 / (1 + 705.654) \\
 &= 70.565.416 / 705.654 \\
 &= 99.99 \\
 &= 100
 \end{aligned}$$

Gambar 3.4. Perhitungan Sampel dengan Rumus Slovin

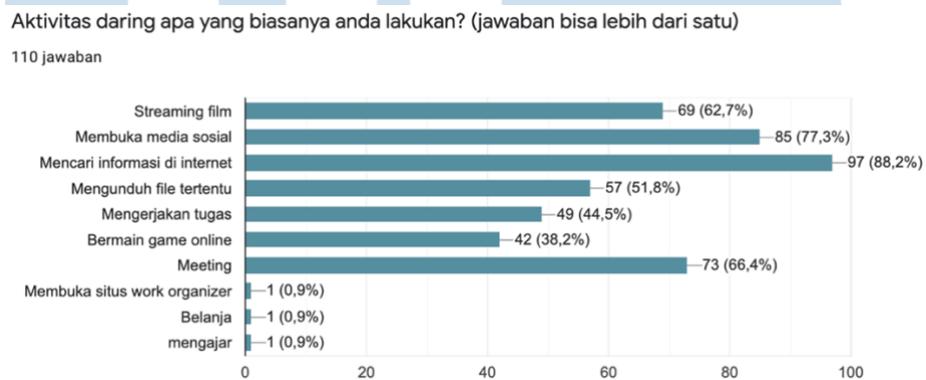
Setelah melakukan perhitungan sampel, penulis menyebarkan kuesioner melalui media sosial kepada kerabat yang memenuhi persyaratan sebagai target responden. Jumlah responden yang didapatkan total ada 110 orang. Adapun hasil kuesioner yang didapatkan adalah sebagai berikut:

Dari skala 1 (sangat jarang) hingga 6 (sangat sering), responden diberikan pilihan untuk menjawab pertanyaan "seberapa sering anda melakukan aktivitas daring?". Dari 110 responden, mayoritas responden menjawab 6 (55,5%), 5 (24,5%) dan 4 (17,3%). Hal ini sudah memperlihatkan bahwa mayoritas responden sangat sering melakukan aktivitas daring, baik menggunakan komputer maupun gawai.



Gambar 3.5. Hasil Respon mengenai Aktivitas Daring

Dari 110 responden yang menjawab pertanyaan "Aktivitas daring apa yang biasanya anda lakukan?", mayoritas responden menjawab mencari informasi di internet (88,2%), membuka media sosial (77,3%), *meeting* 66,4%), *streaming* film (62,7%), mengunduh file tertentu (51,8%). Dapat dilihat dari mayoritas pemilihan jawaban tersebut, responden cenderung melakukan kegiatan yang sangat rentan dan berpotensi menjadi jalan masuknya *malware* pada sebuah perangkat.



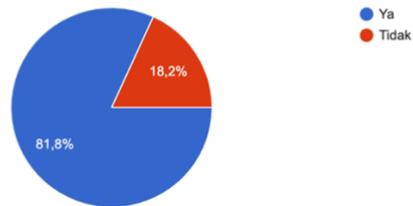
Gambar 3.6. Hasil Respon mengenai Kegiatan Daring

Dari 110 responden, mayoritas sudah pernah mendengar istilah "*malware*" (81,8%), meskipun begitu, sebagian besar responden memiliki pemahaman yang dangkal (49,1%), bahkan sangat dangkal (30%).



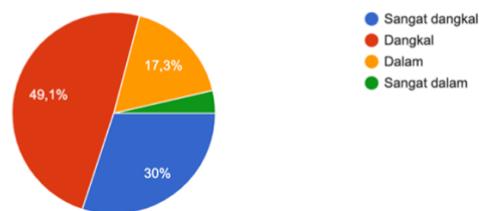
Apakah anda pernah mendengar istilah malicious software (malware)?

110 jawaban



Seberapa dalam pengetahuan anda tentang malware?

110 jawaban

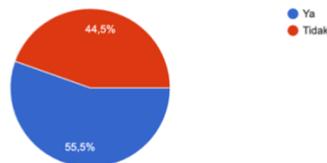


Gambar 3.7. Hasil Respon mengenai Pengetahuan *Malware*

Mayoritas responden pernah mengalami serangan *malware* pada perangkat yang mereka gunakan (55,5%). Meskipun sudah melakukan beberapa tindakan pencegahan seperti tidak mengunduh file sembarangan (78,2%), memasang program *antivirus* (65,5%), dan memilah *email* yang masuk sebelum dibuka (50,9%).

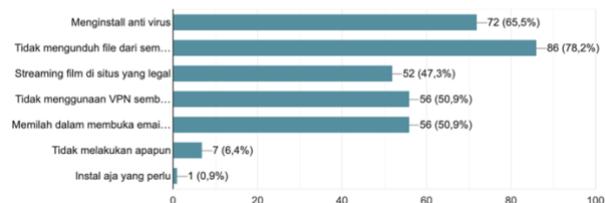
Apakah anda pernah mengalami serangan malware?

110 jawaban



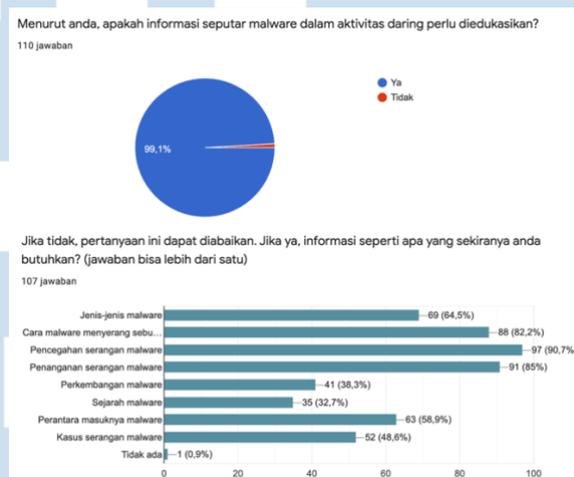
Tindakan pencegahan apa yang sudah anda lakukan dalam pencegahan masuknya malware? (jawaban bisa lebih dari satu)

110 jawaban



Gambar 3.8. Hasil Respon mengenai Pengalaman dan Pencegahan *Malware*

Mayoritas responden merasa edukasi mengenai *malware* perlu diedukasikan (99,1%), terutama mengenai cara pencegahan serangan *malware* (90,7%), penanganan *malware* yang sudah terlanjur menyerang (85%), dan cara *malware* menyerang sebuah perangkat (82,2%).



Gambar 3.9. Hasil Respon mengenai Edukasi *Malware*

Kesimpulan dari hasil kuesioner yang telah penulis lakukan yaitu target responden cenderung sangat sering melakukan aktivitas daring, seperti mencari informasi pada sebuah situs, mengunduh file tertentu, *streaming* film, dan kegiatan lainnya baik menggunakan komputer, laptop, ataupun gawai. Mayoritas responden tahu atau pernah mendengar istilah *malware*, akan tetapi pengetahuan mereka mengenai *malware* masih cukup dangkal. Beberapa responden sudah melakukan tindakan pencegahan masuknya *malware*, terutama dengan menggunakan program *antivirus* pada perangkat mereka, namun masih banyak dari mereka yang terkena serangan *malware* itu sendiri. Edukasi mengenai *malware* menjadi hal yang perlu dilakukan, seperti memberikan informasi tentang tindakan pencegahan serangan *malware*, cara menghapus *malware* yang sudah terlanjur masuk ke dalam sebuah perangkat, cara *malware* masuk ke dalam sebuah perangkat, dan lain sebagainya melalui sebuah media informasi seperti media sosial, website, artikel, atau buku.

3.2 Metode Perancangan

Penulis menggunakan metode perancangan yang berdasar pada buku yang ditulis oleh Landa (2014) yang berjudul *Graphic Design Solutions*. Dalam buku tersebut, metode perancangan dibagi menjadi lima tahap. Mulai dari tahap *orientation, analysis, conception, design, hingga implementation*. Untuk memperoleh metode perancangan yang lebih mendalam, penulis juga menggunakan metode perancangan yang lebih spesifik untuk *website* dalam buku *Ui Design from The Experts: Web Ui Design for Practices*, oleh Bank dan Cao (2015) yang akan penulis masukan pada tahap *design*.

1) *Orientation*

Pada tahap *orientation*, penulis akan melakukan pencarian data, mengumpulkan informasi sebanyak-banyaknya. Mempelajari tentang jenis-jenis malware, menganalisis perkembangan malware, melakukan tinjauan pustaka dibuku atau jurnal yang masih relevan dengan malware, mencari informasi mengetahui pengetahuan masyarakat seputar malware. Kemudian penulis melakukan analisis terhadap data yang telah terkumpul, menentukan target sasaran kampanye, yaitu masyarakat dengan usia 25-34 tahun di daerah Jawa Barat. Lalu mencari tahu media informasi yang serupa untuk mengetahui kelebihan dan kekurangannya. Serta melakukan wawancara kepada ahli digital forensik untuk memastikan data yang dikumpulkan sekaligus memperdalam informasi.

2) *Analysis*

Pada tahap *analysis*, penulis menentukan arah solusi yang akan diambil berdasarkan data-data yang telah dianalisis. Mulai dari memeriksa, menilai, menemukan, dan merencanakan sebuah konsep perancangan. Tahap ini bertujuan agar solusi yang diambil lebih relevan dengan permasalahan yang diangkat. Tahap ini juga dikenal sebagai tahap pembuatan *creative brief*.

3) *Conception*

Pada tahap *conception*, penulis menentukan ide. Ide yang dicari berfungsi untuk menarik minat target terhadap perancangan kampanye, selain untuk ketertarikan, ide yang digunakan juga tetap harus relevan dengan topik permasalahan yang

diangkat. Ide dapat ditemukan dengan beberapa cara, misalnya *brainstorming* atau *mindmapping*.

4) *Design*

Pada tahap *design*, penulis menggunakan metode perancangan oleh Bank dan Cao (2015) dalam bukunya *Ui design from the experts: Web ui design for practices*, yang dimulai dari pembuatan sketsa *website*, melakukan *wireframing* pada setiap halaman *website*, hingga perancangan *prototype*.

a) *Sketch*

Pada tahap ini, penulis merancang visualisasi kasar atau kerangka dari tampilan UI *website* yang akan dirancang, seperti super grafis, logo, dan aset visual lainnya untuk menjadi gambaran dalam melakukan tahap perancangan selanjutnya.

b) *Wireframing*

Pada tahap ini, penulis melakukan beberapa tahap, antara lain sebagai berikut:

(1) Pengaturan konten, *layout*, dan *behavior*

Penulis mempersiapkan konten, tekstual, logo, dan kerangka halaman. Kemudian penulis merancang kerangka *layout*, seperti *header*, *footer*, *branding*, *content area*, dan hirarki. Dan terakhir, penulis merancang *pop up form* dan *error message* untuk membangun *behavior*.

(2) *Low fidelity wireframe*

Penulis merancang *low-fidelity wireframe* sesuai sketsa yang telah dirancang sebelumnya secara lebih detail, dimana sudah memuat komposisi peletakan dari masing-masing elemen visual yang akan digunakan.

(3) *High fidelity wireframe*

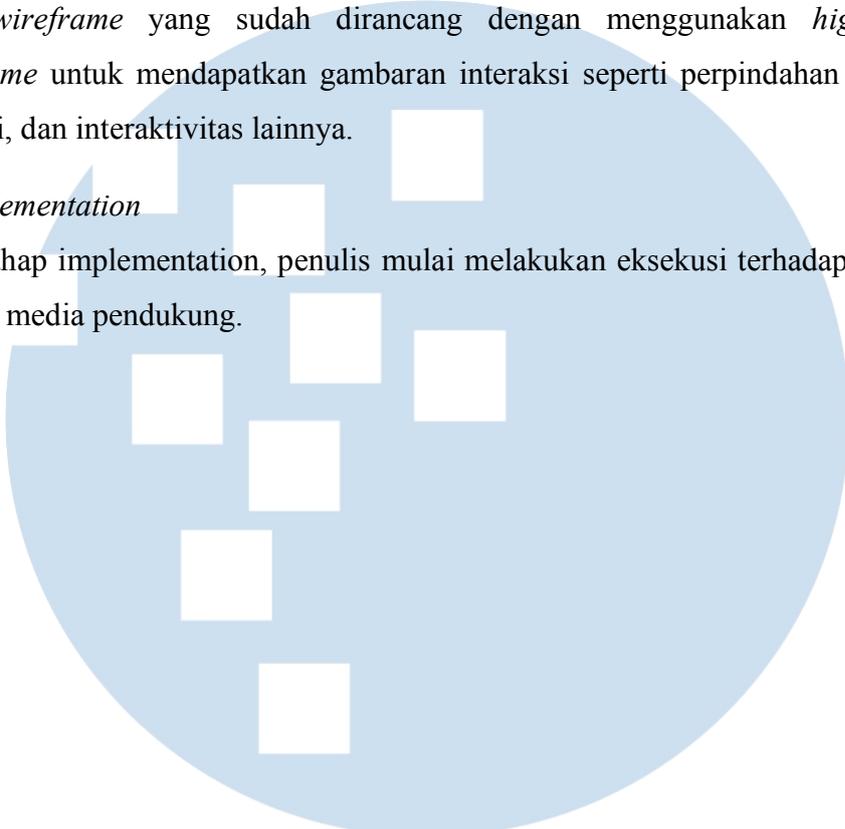
Penulis merancang *high-fidelity wireframe*, dimana pada tahap ini visualisasi perancangan akan sangat detail dan lengkap, untuk memperlihatkan gambaran hasil akhir dari perancangan UI yang telah dibuat.

c) *Prototype*

Pada tahap ini, Penulis menyusun aliran konten saat pengguna membuka *website* pada *wireframe* yang sudah dirancang dengan menggunakan *high-fidelity wireframe* untuk mendapatkan gambaran interaksi seperti perpindahan halaman, animasi, dan interaktivitas lainnya.

5) *Implementation*

Pada tahap *implementation*, penulis mulai melakukan eksekusi terhadap berbagai macam media pendukung.



UMMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA