BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu Yang Relevan

Penelitian terdahulu yang relevan merupakan kumpulan penelitian-penelitian yang pernah dilakukan oleh peneliti sebelumnya yang mempunyai hubungan dengan yang akan dilakukan. Penelitian mengenai *cyber crime* pada pada bank syariah telah banyak diteliti oleh peneliti sebelumnya. Guna membantu dalam penyusunan yang berkaitan dengan analisis pemahaman nasabah internet banking mengenai *cyber crime* pada bank syariah antara lain :

1. Menurut (Pratiwi & Sukarnasih, 2020) dengan judul penelitian "Pengaruh Penggunaan Internet Banking Terhadap *Cyber Crime* Di Masyarakat Denpasar Selatan". Yang dimana hasil penelitian menunjukan bahwa penggunaan internet banking secara partial partial berpengaruh positif yang signifikan terhadap *cybercrime*. Penelitian ini juga menunjukan bahwa perlindungan nasabah pengguna fasilitas internet banking secara partial berpengaruh positif terhadap *cyber crime*. Persamaan penelitian ini dengan penelitian penulis adalah sama-sama meneliti mengenai *cyber crime* di dunia perbankan. Perbedaan penelitian ini dengan penelitian penulis adalah pendekatan yang di gunakan oleh penulis yaitu pendekatan kualitatif sedangkan penelitian ini menggunakan metode kuantitatif internet banking (X1) dan perlindungan nasabah (X2) dan *Cyber crime* (Y).

2. Menurut (Ike Rosandi, 2019) penelitian ini berjudul "Peluang Dan Tantangan Pelayanan Perbankan Melalui Internet Banking dan Mobile Banking" tujuan penelitian ini adalah untuk memberikan pemahaman kepada nasabah mengenai produk mobile banking dan mendampingi nasabah untuk mengunduh dan menginstal aplikasi mobile banking agar minat menggunakan mobile banking meningkat. Berdasarkan kesimpulan dan hasil penelitian ini ditentukan pemahaman yang mempengaruhi minat nasabah dalam menggunakan mobile banking salah satunya adalah faktor kemudahan, keamanan, kenyamanan, efisien dan praktis. faktor yang paling dominan minat nasabah dalam menggunakan mobile banking adalah faktor kenyamanan. Kemudahan dan kemanfaatan juga berpengaruh positif terhadap minat nasabah dalam menggunakan mobile banking. Persamaan penelitian ini adalah sama-sama mengambil penelitian terhadap mobile banking, sedangkan perbedaannya adalah penelitian ini meneliti mengenai peluang dan pelayanan perbankan melalui mobile banking sedangkan penelitian yang saya ambil yaitu analisis pemahaman nasabah mobile banking.

3. Menurut (Syahputra, 2020) penelitian ini berjudul " Analisis Kebijakan Dalam Penaganan Kejahatan *Cyber Crime* (Studi Kasus Cabang Bank BNI Syariah Lhokseumawe" dari penelitian ini faktor-faktor yang mempengaruhi kejahatan *cyber crime* ini seperti kurangnya pendidikan seseorang dimana mengakibatkan seseorang tersebut untuk melakukan tindak kejahatan *cyber crime* agar

mendapatkan penghasilan demi memenuhi kebutuhan sehari-harinya, akses internet yang tidak terbatas, kelalaian pengguna komputer. Persamaan penelitian ini adalah sama-sama menganalisis kejahatan *cyber crime* dengan metode kualitatif. Sedangkan perbedaannya ialah penelitian tersebut mengambil menganalisis kebijakan penanganan kejahatan Cybercrime sedangkan penelitian ini hanya menganalisis pemahaman nasabah mobile banking mengenai Cybercrime.

4. Menurut (Astrini 2015) dengan judul "Perlindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking Dari Ancaman *Cyber Crime*" persaamaan penelitian ini dengan penelitian penulis adalah sama-sama meneliti mengenai *cyber crime*. Adapun jenis perlindungan hukum bagi nasabah dalam dunia perbankan yaitu Upaya dalam mencegah atas keselamatan dan ancaman melalui peraturan perundang-undangan. Upaya ini merupakan upaya hukum untuk menanggulangi keadaan yang tidak diharapkan nantinya oleh nasabah dan Upaya yang bertujuan dalam menyelesaikan sengketa yang timbul atau permasalahan lainnya. Persamaan penelitian ini adalah sama-sama mengambil judul ancaman terhadap *cyber crime*, perbedaannya adalah judul yang saya ambil yaitu menganalisis pemahaman nasabah sedangkan judul dari penelitian ini adalah hukum terhadap pengguna internet banking dari ancaman *cyber crime*.

5. Menurut Hasil Penelitian (Sari, 2021) dengan judul "Pengaruh Prinsip Kehati-Hatian Terhadap Ancaman Situs Phissing Pada Nasabah Penggunaan Internet Banking" pada penelitian ini adalah membahas mengenai ancaman kejahatan yang terjadi terhadap nasabah penggunaan internet banking yang dimana phissing merupakan salah satu ciri *cyber crime* yang terjadi pada pengguna internet banking. Persamaan penelitian ini adalah sama-sama mengambil judul ancaman terhadap *cyber crime*, perbedaannya adalah judul yang saya ambil yaitu menganalisis pemahaman nasabah sedangkan judul dari penelitian ini adalah pengaruh prinsip kehati-hatian terhadap ancaman situs phissing pada nasabah penggunaan internet banking.

2.2 Landasan Teori

2.2.1 Teori Mobile Banking

1. Menurut (Iriani, 2018) mobile banking adalah fasilitas pelayanan dalam pemberian kemudahan akses maupun kecepatan dalam memperoleh informasi terkini dan transaksi finansial secara real time. Mobile banking dapat diakses oleh nasabah perorangan melalui ponsel yang memiliki teknologi GPRS. Produk layanan mobile banking adalah saluran distribusi bank. Untuk mengakses yang memiliki nasabah melalui teknologi GPRS dengan sarana telepon seluler (ponsel).
2. Menurut (Ahmad & Pembudi, 2014) Mobile banking dapat diakses langsung melalui telepon seluler. Saluran ini pada

dasarnya evolusi lebih lanjut dari phone banking, yang memungkinkan nasabah untuk bertransaksi via Hp dengan perintah SMS. Fitur transaksi yang dapat dilakukan yaitu informasi saldo rekening (transfer), pembayaran (kartu kredit, listrik dan telepon), dan pembelian voucher.

3. Mobile banking merupakan sebuah fasilitas dari bank dalam era modern ini mengikuti perkembangan teknologi dan komunikasi. Layanan yang terdapat pada mobile banking meliputi pembayaran,transfer, history dan lain sebagainnya penggunaan mobile banking pada telepon seluler memungkinkan nasabah dapat lebih muda untuk menjalankan aktifitas perbankan berupa batas ruang dan waktu. Dengan adanya layanan moile banking diharapkan dapat memberikan kemudahan dan manfaat bagi seluruh nasabah dalam melakukan akses ke bank tanpa harus datang langsung ke bank.

Jenis-jenis kegiatan mobile banking yaitu:

a. Transfer dana antar rekening atau ke bank lain
b. Informasi saldo dan mutasi rekening
c. Pembayaran tagihan kartu kredit, angsuran, asuransi, rekening listrik, air, telepon TV kabel, kabel dan lain-lain
d. Pembelian tiket transportasi, token listrik, pulsa HP, kuota data dan lain-lain.

Mobile banking dapat diakses langsung melalui telepon seluler. Saluran ini pada dasarnya evolusi lebih lanjut dari phone banking, yang

memungkinkan nasabah untuk bertransaksi via Hp dengan perintah SMS, Fitur transaksi yang dapat dilakukan yaitu informasi saldo rekening (transfer), pembayaran (kartu kredit, listrik dan telepon), dan pembelian voucher.

2.2.2 Teori Pemahaman

Pemahaman berasal dari kata paham yang mempunyai arti mengerti benar, sedangkan pemahaman merupakan proses pembuatan cara memahami (Zul, Fajri, & Senja, 2008). Pemahaman berasal dari kata paham yang artinya pengertian pengetahuan yang banyak, pendapat, pikiran, aliran pandangan, mengerti benar (akan), tahu benar (akan) pandai dan mengerti benar, apabila mendapat imbuhan me-i menjadi memahami, berarti; mengetahui benar, pembuatan, cara memahami atau memahamkan (mempelajari baik-baik supaya paham) sehingga dapat diartikan bahwa pemahaman adalah suatu proses, cara memahami, cara mempelajari baik-baik supaya paham dan mengetahui banyak. Pemahaman dapat dibedakan dalam tiga kategori antara lain :

1. Tingkat terendah adalah pemahaman terjemahan, mulai dari menerjemahkan dalam arti yang sebenarnya, mengartikan prinsip-prinsip
2. Tingkat kedua adalah pemahaman penafsiran, yaitu menghubungkan bagian-bagian terendah dengan yang diketahui berikutnya, atau menghubungkan dengan kejadian, membedakan yang pokok dengan yang bukan pokok.

3. Tingkat ketiga merupakan tingkat tertinggi yaitu pemahaman ektrapolasi.

Pemahaman adalah suatu hal yang kita mengerti dengan benar. Pemahaman merupakan salah satu bentuk hasil belajar. Pemahaman ini terbentuk akibat dari adanya proses belajar. Kemampuan seseorang dalam memahami menjadi bagian penting dalam mengetahui atau mempelajari sesuatu. Seseorang memiliki pengetahuan atau mengetahui sesuatu, namun belum pasti ia memahaminya. Tetapi, seseorang yang memiliki pemahaman sudah tentu ia mengetahuinya. Pemahaman juga dapat dikatakan sebagai cara seseorang dalam menentukan arti informasi. Kemudian akan menciptakan pengetahuan dan kepercayaan secara personal setelah proses pemahaman selesai maka akan diikuti keinginan untuk mempelajari dan melakukan timbal balik dengan baik terhadap objek yang ada.

Pemahaman merupakan kemampuan untuk menggunakan pengetahuan yang sudah dilihat kurang lebih sama dengan yang sudah diajarkan dan sesuai dengan maksud penggunaanya.

Pemahaman bukan kegiatan berfikir semata, melainkan pemindahan letak dari dalam berdiri disituasi atau dunia orang lain. Mengalami kembali situasi yang dijumpai pribadi lain di dalam erlebnis(sumber pengetahuan tentang hidup, kegiatan melakukan pengalaman pikiran), pemahaman yang terhayati. Pemahaman merupakan suatu kegiatan berfikir secara diam-diam, menemukan dirinya dalam orang.

Memahami adalah mengetahui tentang sesuatu dan dapat melihatnya dari berbagai segi. Pemahaman merupakan jenjang kemampuan berpikir yang setingkat lebih tinggi dari ingatan dan hafalan. Dengan kata lain dapat disimpulkan bahwa pemahaman dapat diartikan mengerti tentang sesuatu dan dapat melihatnya dari berbagai segi. Jadi seseorang baru dikatakan memahami sesuatu apabila dia dapat menangkap intinya serta memberikan penjelasan kepada orang lain dengan baik atau uraian yang lebih rinci.

Menurut (Kuswana, 2012, h. 18) Pemahaman memiliki 5 indikator yaitu:

1. Menjelaskan kembali

   Menjelaskan kembali adalah seorang yang sudah selesai mempelajari sesuatu maka, seseorang akan mampu menjelaskan kembali materi yang dipelajari.
2. Menguraikan dengan kata-kata sendiri.

   Menguraikan dengan kata-kata sendirimerupakan setelah selesai proses pembelajaran maka seseorang akan mampu menguraikan kembali materi yang telah disampaikan dengan menggunakan kata-kata sendiri, dengan demikian seseorang akan menjelaskan kembali dengan kata yang berbeda namun memiliki makna yang sama.
3. Merangkum

   Merangkum adalah seseorang mampu meringkas uraian dari pendidikan maupun anggota kelompok dalam proses diskusi tanpa mengurangi kandungan makna yang ada dalam materi.

4. Memberikan contoh

   Memberikan contoh merupakan apabila seseorang yang telah menyelesaikan pembelajarannya mereka mampu memberikan contoh pada suatu peristiwa yang berkaitan dengan materi dari penjelasan yang ada akan dikembangkan melalui contoh-contoh yang lebih nyata dalam kehidupan yang dialami.

5. Menyimpulkan

   Menyimpulkan merupakan seseorang yang mempelajari sesuatu akan mampu menemukan inti yang paling mendasar dari materi yang dipelajari.

2.2.3. Teori *Cyber Crime*

Sebagai makhluk tuhan yang mempunyai unsur fisik (jasad) dan non fisik (jiwa, pikiran, nafsu, dsb), manusia dalam kehidupan juga mempunyai berbagai tujuan hidup dan obsesi yang hendak diraihnya. Namun semua yang hendak dicapai itu harus menyesuaikan dengan jalan Tuhan. Dalam artian manusia sebisanya harus menyeimbangkan unsur ragawi, indrawi, dan rohani.

Manusia pada awalnya diciptakan Oleh Allah dalam keadaan fitrah, namun sejatinya manusia diberikan potensi oleh Allah untuk menjaga dirinya sehingga tetap berada dalam kondisi fitrah tersebut, juga diberikan potensi untuk mengotori fitrahnya. Dalam Q.S. Al-Syams [91]: 7-10, Allah berfirman :

وَنَفْسٍ وَمَا سَوَّاهَا (7) فَأَلْهَمَهَا فُجُورَهَا وَتَقْوَاهَا (8) قَدْ مَنْ أَفْلَحَ زَكَّاهَا (9) وَقَدْ خَابَ مَنْ دَسَّاهَا (10)

Terjemahannya :

"Dan jiwa serta penyempurnaannya (ciptaannya). Maka Allah mengilhamkan kepada jiwa itu (jalan) kefasikan dan ketakwaannya. Sesungguhnya beruntunglah orang yang mensucikan jiwa itu. Dan sesungguhnya merugilah orang yang mengotorinya." Q.S. Al-Syams [91]: 7-10.

Oleh karena itu manusia diberi akal agar bisa membedakan mana yang baik dan mana yang buruk dan mampu mengarahkan dirinya menuju kebaikan atau keburukan dalam kadar yang sama. Oleh karena itu tidaklah mengherankan apabila dalam kehidupan ini banykan di jumpai kejahatan yang dilakukan oleh manusia. (Muhammadun, 2011)

Adanya kejahatan siber (*Cyber crime*) telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet. Hal ini merupakan akibat dari pesatnya perkembangan teknologi informasi, sehingga setiap perkembangan pada hakikatnya membawa efek seperti dua sisi mata uang yang masing-masing saling berkaitan dan tidak terpisahkan, yang berupa sisi positif dan sisi negatif. Kejahatan siber bermula dari kehidupan masyarakat yang ikut memanfaatkan dan cenderung meningkat setiap saat untuk berkonsentrasi dalam *cyberspace.* Hal ini merupakan bagian dari makin majunya perkembangan zaman, makin sarat pula beban sosial dan beban kriminalitas dalam bermasyarakat. Perkembangan ini membawa dampak pada kehidupan sosial dari masyarakatnya, dilain pihak pada tingkat kemajuan yang sedang dialami, juga membawa dampak timbulnya berbagai bentuk kejahatan. (Janggih & Qamar, 2018)

Cyber crime adalah istilah yang mengacu pada aktifitas kejahatan dengan komputer atau jarinagan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termaksud kejahatan *cyber crime* adalah penipuan kartu kredit, pemalsuan cek, pornografi anak, penipuan identitas dan sebagainya. Walaupun kejahatan *cyber crime* pada umumnya mengacu kepada aktifitas kejahaatn atau jaringan komputer sebagai unsur utamanya istilah ini juga digunakan untuk kegiatan tradisional dimana komputer atau jarinagan komputer digunakan untuk mempermudah atau memungkinkan kegiatan itu terjadi.

Kejahatan *cyber crime* merupakan jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi tanpa batas serta memiliki karakteristik yang kuat dengan rekayasa teknologi yang mengandalkan pada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelannggan internet.

Direktur Kebijakan Dan Pengawasan Sistem Pembayaran BI Ida Nuryanti mengatakan bahwa ada sejumlah modus kejahatan perbankan atau *cyber crime* yang sering kali yaitu berupa kejahatan malware, phissing, skimming malware yaitu kejahatan perbankan atau *cyber crime* yang sering kali terjadi yaitu singkronisasi token, dimana sistem bank diserang yakni device media komunikasi yang sering digunakan pengguna. Phissing merupakan upaya pencurian informasi nasabah user id, kata sandi maupun password rekening maupun kartu kredit,. Jadi ada website yang mirip dengan website aslinya dimana kita diminta untuk memasukan nomor rekening beserta password. Sedangkan skimming adalah tindak pencurian data nasabah dengan menggunakan

alat perekam data. Biasanya kejahatan ini dilakukan di mesin anjungan tunai mandiri EDC. Dengan chip belum terbukti bisa di skimming. Kartu kredit sudah ada chipnya, sekarang yang masih proses situs kartu debit beralih chip.

Dalam arti sempit *cyber crime* adalah computer crime yang ditunjukan terhadap sistem atau jaringan komputer, sedangkan dalam arti luas, *cyber crime* mencakup seluruh bentuk baru kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan hanya bantuan peralatan komputer (*komputer relate crime*). Kegiatan yang potensial menjadi target *cyber crime* dalam kegiatan perbankan antara lain adalah :

1. Layanan pembayaran menggunakan kartu kredit pada situs-situs toko online
2. Layanan perbankan online (*online banking*).

Menurut (Rahma, 2018) modus yang pernah muncul di Indonesia dikenal dengan istilah *typosite* memanfaatkan kelengahan nasabah yang salah dalam mengetikan alamat bank yang akan di akses. Pelakunya sudah menyiapkan situs palsu yang mirip dengan situs aslinya. Jika ada nasabah yang salah mengetik dan masuk ke dalam situs palsu tersebut, maka pelaku akan merekam ID dan password nasabah tersebut untuk digunakan mengakses situs yang sebenarnya (illegal acsess) dengan maksud untuk merugikan nasabah, beberapa potensi *cyber crime* pada kegiatan perbankan antara lain :

1. *Typo site*, pelaku membuat nama situs palsu yang sama persis dengan situs asli dan membuat alamat yang mirip dengan alamat situs asli. Pelaku menunggu kesempatan jika seseorang korban salah mengetikkan alamat dan masuk ke situs palsu buatannya. Jika hal ini terjadi maka pelaku akan memperoleh informasi user dan password korbannya, dan dapat dimanfaatkan untuk merugikan korban.
2. *Keylogger/keystroke logger*, Modus lainnya adalah *keylogger*. Hal ini sering terjadi pada tempat mengakses internet umum seperti di warnet. Program ini akan merekam karakter-karakter yang diketikkan oleh user dan berharap akan mendapatkan data penting seperti user ID maupun *password*. Semakin sering mengakses internet di tempat umum, semakin rentan pula terkena modus operandi yang dikenal dengan istilah *keylogger* atau *keystroke recorder* ini. Sebab komputer-komputer yang ada di warnet digunakan berganti-ganti oleh banyak orang. Cara kerja dari modus ini sebenarnya sangat sederhana, tetapi banyak para pengguna komputer ditempat umum yang lengah dan tidak sadar bahwa semua aktifitasnya dicatat oleh orang lain. Pelaku memasang program *keylogger* di komputer-komputer umum, program keylogger ini akan merekam semua tombol keyboard yang ditekan oleh pengguna komputer berikutnya. Di lain waktu, pemasang *keylogger* akan mengambil hasil "jebakannya" dikomputer yang sama, dan dia berharap akan memperoleh informasi penting dari para korbannya, semisal user ID dan *password*.

3. *Sniffing*, usaha untuk mendapatkan user ID dan *password* dengan jalan mengamati paket data yang lewat pada jaringan komputer.
4. *Brute Force Attacking*, usaha untuk mendapatkan *password* atau *key* dengan mencoba semua kombinasi yang mungkin.
5. *Web Deface: System Exploitation* dengan tujuan mengganti tampilan halaman muka satu situs.
6. *Email Spamming*, mengirimkan junk email berupa iklan produk dan sejenisnya pada alamat email seseorang.
7. *Daniel of Service*, membanjiri data dalam jumlah sangat besar dengan maksud untuk melumpuhkan sistem sasaran.
8. *Virus worm, Trojan*, menyebarkan virus *worm* maupun Trojan dengan tujuan untuk melumpuhkan sistem komputer, memperoleh data-data dari sistem korban dan untuk mencemarkan nama baik pembuat perangkat lunak tertentu.

Contoh *cyber crime* dalam transaksi perbankan yang menggunakan sarana internet sebagai basis transaksi adalah sistem layanan kartu kredit dan layanan perbankan online/online banking. Dalam sistem layanan yang pertama, yang perlu diwaspadai adalah tindak kejahatan yang dikenal dengan istilah *carding*. Prosesnya adalah sebagai berikut, pelaku *carding* memperoleh data kartu kredit korban secara tidak sah, dan kemudian menggunakan kartu kredit korban tersebut untuk berbelanja di toko online . modus ini dapat terjadi akibat lemahnya sistem autentifikasi yang digunakan dalam memastikan identitas pemesanan barang ditoko online.

Cyber crime dapat menyebabkan hal-hal dibawah ini yaitu :

a. Terjadinya cyber crime pada nasabah
b. Bentuk ganti rugi dari bank
c. Kepercayaan nasabah
d. Tindak lamjut pihak bank
e. Perlindungan dari kejahatan cyebr
f. Peraturan yang berlaku

Dapat diketahui terdapat beberapa jenis-jenis dari *cyber crime* bila dilihat dari aktivitasnya, yaitu sebagai berikut:

a. *Carding* adalah berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, biasanya dengan mencuri data di internet. Sebutan pelakunya adalah "*carder*". Sebutan lain untuk kejahatan jenis ini adalah *cyberfroud* alias penipuan di dunia maya.
b. *Hacking* adalah menerobos program komputer milik orang/pihak lain. *Hacker* adalah orang yang gemar ngoprek komputer, memiliki keahlian membuat dan membaca program tertentu dan terobsesi mengamati keamanan (*security*)-nya.
c. *Cracking* adalah *hacking* untuk tujuan jahat. Sebutan untuk "*cracker*" adalah "*hacker*" bertopi hitam (*black hat hacker*). Berbeda dengan "*carder*" yang hanya mengintip kartu kredit, "*cracker*" mengintip simpanan para nasabah di berbagai bank atau pusat data sensitif lainnya untuk keuntungan diri sendiri. Meski sama-sama menerobos keamanan komputer orang lain,

hacker lebih fokus pada prosesnya. Sedangkan *cracker* lebih fokus untuk menikmati hasilnya.

d. *Defacing* adalah kegiatan mengubah halaman situs/website pihak lain, seperti yang terjadi pada situs Menkominfo dan Partai Golkar, BI baru-baru ini dan situs KPU saat pemilu 2004 lalu. Tindakan *deface* ada yang semata-mata iseng, unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga yang jahat, untuk mencuri data dan dijual kepada pihak lain.
e. *Phissing* adalah kegiatan memancing pemakai komputer di internet (*user*) agar mau memberikan informasi data diri pemakai (*username*) dan kata sandinya (*password*) pada suatu website yang sudah di-deface. *Phissing* biasanya diarahkan kepada pengguna online banking. Isian data pemakai dan *password* yang vital.
f. *Spamming* adalah pengiriman berita atau iklan lewat surat elektronik (e-mail) yang tak dikehendaki. Spam sering disebut juga sebagai bulk e-mail atau junk e-mail alias "sampah".
g. *Malware* adalah program komputer yang mencari kelemahan dari suatu software.Umumnya malware diciptakan untuk membobol atau merusak suatu software atau operating system. *Malware* terdiri dari berbagai macam, yaitu: virus, worm, trojan horse, adware, browser hijacker dan lain-lain.

2.3 Grand Teory

Menurut (Kuswana, 2012) terdapat tujuh indikator pemahaman antara lain :

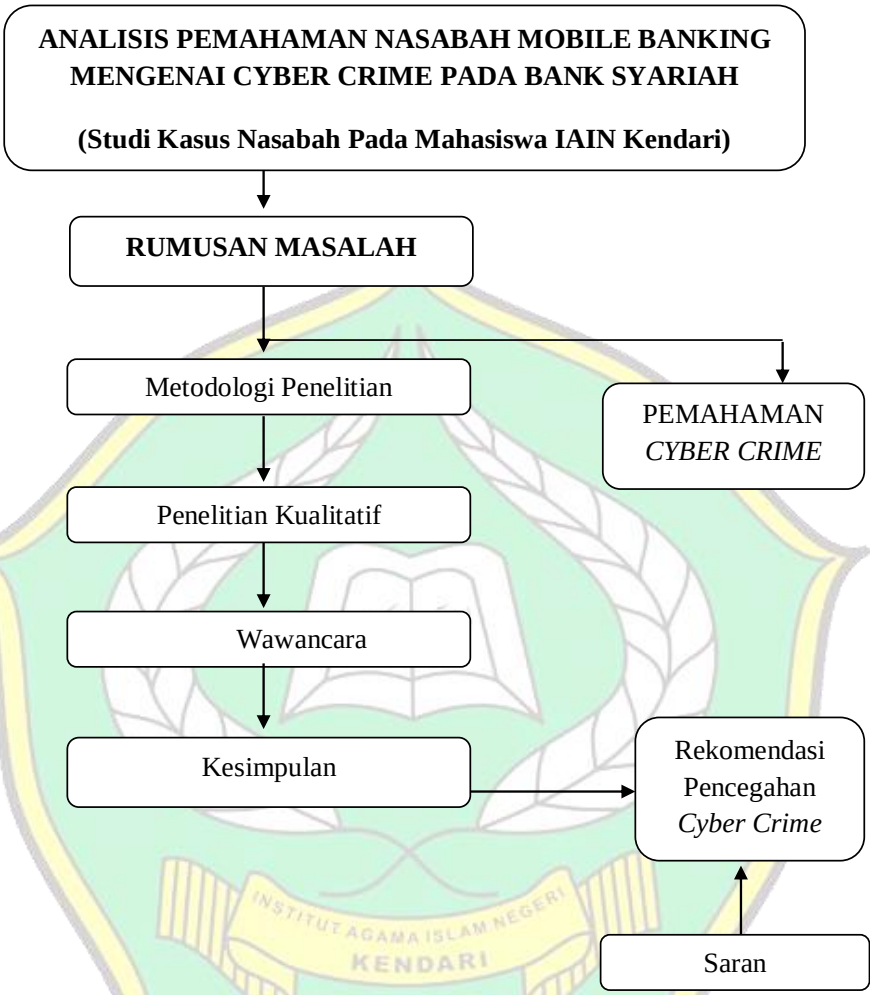
1. Menjelaskan kembali
2. Menguraikan dengan kata-kata sendiri
3. Merangkum
4. Memberikan contoh
5. Menyimpulkan

Menurut (Rahma, 2018) terjadinya *cyber crime* dapat menyebabkan hal-hal dibawah ini yaitu :

1. Terjadinya *cyber crime* pada nasabah
2. Bentuk ganti rugi dari bank
3. Kepercayaan nasabah
4. Tindak lanjut pihak bank
5. Perlindungan dan kejahatan *cyber*
6. Peraturan yang berlaku

2.4 Kerangka Pikir

Kerangka Pikir adalah pemahaman yang sangat mendasar yang menjadi landasan bagi pemahaman-pemahaman setiap pemikir selanjutnya. Kerangka berfikir berbeda dengan sekumpulan informasi atau hanya sekedar sebuah pemahaman. Lebih dari itu kerangka berfikir adalah sebuah pemahamn yang melandasi pemahaman-pemahaman yang lainnya, sebuah pemikiran yang sangat mendasar yang menjadi pondasi setiap pemikiran berikutnya.


ANALISIS PEMAHAMAN NASABAH MOBILE BANKING MENGENAI CYBER CRIME PADA BANK SYARIAH
(Studi Kasus Nasabah Pada Mahasiswa IAIN Kendari)
RUMUSAN MASALAH
Metodologi Penelitian
Penelitian Kualitatif
Wawancara
Kesimpulan
PEMAHAMAN CYBER CRIME
Rekomendasi Pencegahan Cyber Crime
Saran