ANALISIS KEBIJAKAN DALAM PENANGANAN KEJAHATAN *CYBER CRIME* (STUDI KASUS CABANG BANK BNI SYARIAH LHOKSEUMAWE)

Disusun Oleh:

AIDIL SYAHPUTRA
NIM. 140603132

PROGRAM STUDI PERBANKAN SYARIAH

FAKULTAS EKONOMI DAN BISNIS ISLAM

UNIVERSITAS ISLAM NEGERI AR-RANIRY

BANDA ACEH

2020/1441 H

LEMBAR PERNYATAAN KEASLIAN KARYA ILMIAH

Yang bertandatangan di bawah ini

Nama	: Aidil Syahputra
NIM	: 140603132
Program Studi	: Perbankan Syariah
Fakultas	: Fakultas Ekonomi dan Bisnis Islam

Dengan ini menyatakan bahwa dalam penulisan SKRIPSI ini, Saya:

1. ***Tidak menggunakan ide orang lain tanpa mampu mengembangkan dan mempertanggungjawabkan.***
2. ***Tidak melakukan plagiasi terhadap naskah karya orang lain.***
3. ***Tidak menggunakan karya orang lain tanpa menyebutkan sumber asli atau tanpa izin pemilik karya.***
4. ***Tidak melakukan pemanipulasian dan pemalsuan data.***
5. ***Mengerjakan sendiri karya ini dan mampu mempertanggungjawabkan atas karya ini.***

Bila di kemudian hari ada tuntukan dari pihak lain atas karya saya, dan telah melalui pembuktian yang dapat di pertanggungjawabkan dan ternyata memang ditemukan bukti bahwa saya telah melanggar pernyataan ini, maka saya siap untuk dicabut gelar akademik saya atau diberikan sanksi lain berdasarkan aturan yang berlaku di Fakultas Ekonomi dan Bisnis Islam UIN Ar-Raniry.

Demikian pernyataan ini saya buat dengan sesungguhnya.

Banda Aceh, 27 Juli 2020
Yang Menyatakan,

Aidil Syahputra
NIM. 140603132

LEMBAR PERSETUJUAN SIDANG SKRIPSI

SKRIPSI

Diajukan Kepada Fakultas Ekonomi dan Bisnis Islam UIN Ar-Raniry Banda Aceh Sebagai Salah Satu Beban Studi Untuk Menyelesaikan Program Studi Perbankan Syariah

Dengan Judul:

Analisis Kebijakan Dalam Penanganan Kejahatan *Cyber Crime* (Studi Kasus Cabang Bank BNI Syariah Lhokseumawe)

Disusun Oleh:

Aidil Syahputra
NIM. 140603132

Disetujui untuk diseminarkan dan dinyatakan bahwa isi dan formatnya telah memenuhi syarat sebagai kelengkapan dalam penyelesaian studi pada Program Studi Ilmu Ekonomi Fakultas Ekonomi dan Bisnis Islam UIN Ar-Raniry

Pembimbing I,	Pembimbing II.
Muhammad Arifin, Ph. D	Cut Elfida, S.H.I., M.A
NIP. 1974105 200604 1 002	NIDN. 2012128901

Mengetahui
Ketua Program Studi Ilmu Ekonomi,

Dr. Nevi Hasnita, M.Ag
NIP. 197711052006042093

LEMBAR PENGESAHAN SIDANG HASIL SKRIPSI

Aidil Syahputra
NIM. 14060132

DenganJudul:

Analisis kebijakan Dalam Penanganan Kejahatan *Cyber crime* (Studi kasus Bank BNI Syariah Lhokseumawe)

Telah Diseminarkan Oleh Program Studi Strata Satu (S1)
Fakultas Ekonomi dan Bisnis Islam UIN Ar-Raniry dan Dinyatakan Lulus Serta Diterima Sebagai Salah Satu Beban Studi Untuk Menyelesaikan Program Studi Strata 1 dalam bidang Perbankan Syariah

Pada Hari/Tanggal : Senin, 27 Juli 2020
6 Zulhijah 1441 H

Banda Aceh
Tim Penilai Sidang Hasil Skripsi

Ketua,	Sekretaris,
Muhammad Arifin, Ph. D	Cut Elfida, SHI., MA
NIP. 197410152006041002	NIDN. 2012128901
Penguji I,	**Penguji II,**
Dr.Israk Ahmadsyah,B.Ec.,M.Sc	Riza Aulia, S. E.I, MSc
NIP. 197209072000031001	NIP. 198801302018031001

Mengetahui
Dekan Fakultas Ekonomi dan Bisnis Islam
UIN Ar-Raniry Banda Aceh

Dr. Zaki Fuad, M.Ag
NIP. 196401419 2031003

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITASISLAM NEGERI AR-RANIRY BANDA ACEH
UPT. PERPUSTAKAAN
Jl. Syeikh Abdur Rauf Kopelma Darussalam Banda Aceh
Telp. 0651-7552921, 7551857, Fax. 0651-7552922
Web :www.library.ar-raniry.ac.id, Email : library@ar-raniry.ac.id

FORM PERNYATAAN PERSETUJUAN PUBLIKASIKARYA ILMIAH MAHASISWA UNTUK KEPENTINGAN AKADEMIK

Saya yang bertanda tangan di bawah ini:

Nama Lengkap	: Aidil Syahputra
NIM	: 140603132
Fakultas/Jurusan	: Ekonomi dan Bisnis Islam/Perbankan Syariah
E-mail	: aidilputra173@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada UPT Perpustakaan Universitas Islam Negeri (UIN) Ar-Raniry Banda Aceh, Hak Bebas Royalti Non-Eksklusif (*Non-exclusive Royalty-Free Right*) atas karya ilmiah :

☐ Tugas Akhir ☐ KKU ☐ Skripsi ☐ .....

yang berjudul:

Analisis kebijakan Dalam Penanganan Kejahatan *Cyber crime* (Studi kasus Bank BNI Syariah Lhokseumawe).

Beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Eksklusif ini, UPT Perpustakaan UIN Ar-Raniry Banda Aceh berhak menyimpan, mengalih-media formatkan, mengelola, mendiseminasikan, dan mempublikasikannya di internet atau media lain. Secara *fulltext* untuk kepentingan akademik tanpa perlu meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis, pencipta dan atau penerbit karya ilmiah tersebut.

UPT Perpustakaan UIN Ar-Raniry Banda Aceh akan terbebas dari segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian peryataan ini yang saya buat dengan sebenarnya.
Dibuat di : Banda Aceh
Pada tanggal : 3 Februari 2021

Mengetahui,

Penulis	Pembimbing I	Pembimbing II
Aidil Syahputra	Muhammad Arifin, Ph. D	Cut Elfida, SHI., MA
140603132	NIP: 197209072000031001	NIDN. 2012128901

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Alhamdulillah, puji syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan Skripsi ini. Shalawat dan salam penulis sanjungkan kepangkuan Nabi Muhammad SAW, beserta keluarga dan sahabat beliau yang telah memberikan pencerahan bagi kita hingga dapat merasakan nikmatnya iman dalam Islam, serta nikmat kemuliaan dalam ilmu pengetahuan.

Penulisan Skripsi ini yang berjudul "**Analisis Kebijakan Dalam Penanganan Kejahatan *Cyber Crime* (Studi Kasus Cabang Bank BNI Syariah Lhokseumawe)**" untuk melengkapi salah satu persyaratan dalam menyelesaikan studi pada Program S1 Perbankan Syariah UIN Ar-Raniry Banda Aceh. Dalam penyusunan Skripsi ini, penulis mendapat bimbingan, arahan dan bantuan dari banyak pihak. Oleh karena itu, penulis menyampaikan ungkapan terima kasih kepada:

1. Bapak Dr. Zaki Fuad, M. Ag, selaku Dekan Fakultas Ekonomi dan Bisnis Islam
2. Ibu Nevi Hasnita, S.Ag., M.Ag selaku Ketua Prodi Perbankan Syariah, dan Ibu Ayumiati, S.E., M.Si, selaku Seketaris Prodi Perbankan Syariah yang telah memberikan nasehat-nasehat, arahan dan bimbingan dalam menyelesaikan skripsi ini.

3. Bapak Muhammad Arifin, Ph. D selaku Ketua Laboratorium Fakultas Ekonomi dan Bisnis Islam UIN Ar-Raniry, dan juga selaku pembimbing I yang telah memberikan kemudahan dan dukungan sehingga terselesaikan skripsi ini. Dan Ibu Cut Elfida, S.H.I., M.A selaku pembimbing II yang telah memberikan motivasi, bimbingan dan pengarahan dalam penyusunan skripsi ini.
4. Ibu Jalilah, S. HI.,M. Ag selaku penasehat Akademik yang telah memberikan bimbingan dan arahan selama kuliah.
5. Orang tua terhebat yang penulis cintai, Ayahanda Abdul Gani Ali dan Ibunda Rukiah S.Pd yang senantiasa mendidik, memberi dukungan dan doa kepada penulis.
6. Sahabat-sahabatku tercinta (Rahazard, Azharni, Azhari, Agos, Sry Wahyuni, Yuyun, Mutia Riska, Mimi, Cut Hasna, Zul Ridha, Nafisah, Ariski, Rafi Mustafa, Muhib, Fadlon, Fadli, Tunis, Kenzo, Nanda Ulfa, Jal, Munirwan, Nurzahraini, Khalik Akmal, Feri Andista, Fahmi, Nazar Maulana, Ikhsan, Riski Muksalmina, Muksal, Zia Ulhaq, Asyraf, Munazir, Fadil, Putra, Mahfud, Danil, Bella, Fira, Kania Ulfa, Arifuddin, Khairon, Khairun Sabri, Juni Irayana, Gusvi Rosa, Listanti, dan Aya) yang telah memberikan semangat dan dukungan kepada penulis.

Meskipun segala usaha telah dilakukan untuk penyempurnaan Skripsi ini, namun penulis menyadari masih banyak kekurangan baik dari segi penulisan maupun pembahasannya. Penulis sangat

mengharapkan kritik dan saran yang membangun demi meningkatkan mutu dan menyempurnakan penyusunan Skripsi ini kedepannya.

Semoga kita selalu mendapatkan Ridha dan Rahmat dari Allah SWT, *Amin YaaRabbal'Alamin*.

Banda Aceh, 20 Januari 2021

Penulis,

Aidil Syahputra

TRANSLITERASI ARAB-LATIN DAN SINGKATAN

Keputusan Bersama Menteri Agama dan Menteri P dan K
Nomor: 158 Tahun 1987 – Nomor: 0543 b/u/1987

1. Konsonan

No	Arab	Latin	No	Arab	Latin
1	ا	Tidak dilambangkan	16	ط	T
2	ب	B	17	ظ	Z
3	ت	T	18	ع	‘
4	ث	Ṡ	19	غ	G
5	ج	J	20	ف	F
6	ح	Ḥ	21	ق	Q
7	خ	Kh	22	ك	K
8	د	D	23	ل	L
9	ذ	Ż	24	م	M
10	ر	R	25	ن	N
11	ز	Z	26	و	W
12	س	S	27	ه	H
13	ش	Sy	28	ء	’
14	ص	Ṣ	29	ي	Y
15	ض	Ḍ			

2. Vokal

Vokal Bahasa Arab, seperti vokal bahasa Indonesia, terdiri dari vokal tunggal atau monoftong dan vokal rangkap atau diftong.

a. Vokal Tunggal

Vokal tunggal bahasa Arab yang lambangnya berupa tanda atau harkat, transliterasinya sebagai berikut:

Tanda	Nama	Huruf Latin
◌َ	*Fatḥah*	a
◌ِ	*Kasrah*	i
◌ُ	*Dammah*	u

b. Vokal Rangkap

Vokal rangkap bahasa Arab yang lambangnya berupa gabungan antara harkat dan huruf, transliterasinya gabungan huruf, yaitu:

Tanda dan Huruf	Nama	Gabungan Huruf
◌َ ي	*Fatḥah* dan ya	ai
◌َ و	*Fatḥah* dan wau	au

Contoh:

كيف : *kaifa* هول: *haula*

3. *Maddah*

Maddah atau vokal panjang yang lambangnya berupa harkat dan huruf, transliterasinya berupa huruf dan tanda, yaitu:

Harkat dan Huruf	Nama	Huruf dan tanda
ي /اَ	*Fatḥah* dan *alif* atau ya	Ā
ِي	*Kasrah* dan ya	Ī
ُي	*Dammah* dan wau	Ū

Contoh:

قَالَ: *qāla*

رَمَى : *ramā*

قِيْلَ : *qīla*

يَقُوْلُ : *yaqūlu*

4. Ta *Marbutah* (ة)

Transliterasi untuk ta marbutah ada dua.

a. Ta *marbutah* (ة) hidup
Ta *marbutah* (ة) yang hidup atau mendapat harkat *fatḥah*, *kasrah* dan *dammah*, transliterasinya adalah t.

b. Ta *marbutah* (ة) mati
Ta *marbutah* (ة) yang mati atau mendapat harkat sukun, transliterasinya adalah h.

c. Kalau pada suatu kata yang akhir katanya ta *marbutah* (ة) diikuti oleh kata yang menggunakan kata sandang al, serta bacaan kedua kata itu terpisah maka ta *marbutah* (ة) itu ditransliterasikan dengan h.

Contoh:

رَوْضَةُ اْلَاطْفَالْ : *rauḍah al-aṭfāl/ rauḍatul aṭfāl*

اَلْمَدِيْنَةُ الْمُنَوَّرَةْ	: *al-Madīnah al-Munawwarah/ al-Madīnatul Munawwarah*
طَلْحَةْ	: *Ṭalḥah*

Catatan:

Modifikasi

1. Nama orang berkebangsaan Indonesia ditulis seperti biasa tanpa transliterasi, seperti M. Syuhudi Ismail, sedangkan nama-nama lainnya ditulis sesuai kaidah penerjemahan. Contoh: Ḥamad Ibn Sulaiman.
2. Nama negara dan kota ditulis menurut ejaan Bahasa Indonesia, seperti Mesir, bukan Misr; Beirut, bukan Bayrut; dan sebagainya.
3. Kata-kata yang sudah dipakai (serapan) dalam kamus Bahasa Indonesia tidak ditransliterasi. Contoh: Tasauf, bukan Tasawuf.

ABSTRAK

Nama : Aidil Syahputra
NIM : 140603132
Fakultas/Prodi : Fakultas Ekonomi dan Bisnis Islam
Judul Skripsi : Analisis Kebijakan Dalam Penanganan Kejahatan *Cyber Crime* (Studi Kasus Bank BNI Syariah Lhokseumawe)
Pembimbing I : Muhammad Arifin, Ph. D
Pembimbing II : Cut Elfida, S.H.I., M.A

Cyber crime merupakan suatu aktivitas kejahatan di dunia maya dengan memanfaatkan jaringan komputer sebagai alat dan jaringan internet sebagai medianya. Tujuan penelitian ini adalah mengetahui faktor- faktor yang menyebabkan kejahatan *cyber crime* di Bank BNI Syariah Lhokseumawe, dan mengetahui kebijakan Bank BNI Syariah dalam menangani kejahatan *cyber crime* tersebut. Metode yang digunakan dalam penelitian ini yaitu metode kualitatif. Hasil penelitian menunjukkan bahwa faktor-faktor yang mempengaruhi kejahatan *cyber crime* dibagi menjadi 2 kategori: kejahatan yang menjadikan sistem dan jaringan komputer sebagai sarana kejahatan dan kejahatan yang menggunakan komputer sebagai sarana, kedua kategori kejahatan tersebut dikenal dengan istilah kejahatan yang berhubungan dengan computer (*computer-related crime*).

Kata kunci : *Cyber Crime*, Kejahatan, internet dan Komputer

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan ilmu pengetahuan dan teknologi telah memberikan dampak yang sangat positif bagi peradaban umat manusia. Salah satu fenomena abad modern yang sampai saat ini masih terus berkembang dengan pesat adalah internet. Pada mulanya jaringan internet hanya dapat digunakan oleh lingkungan pendidikan (perguruan tinggi) dan lembaga penelitian. Namun saat ini jaringan internet juga sudah marak digunakan pada dunia bisnis, baik di tingkat lokal maupun global dari cara mengumpulkan data untuk merekrut karyawan pada perusahaan, cara bisnis menggunakan internet sangat banyak, sebagai manfaat dari internet untuk komunitas bisnis. Orang telah menemukan berbagai manfaat internet untuk bisnisnya. Banyak perusahaan kecil dan besar telah memanfaatkan internet demi menunjang bisnis mereka. Bahkan ada yang dinamakan bisnis *online* dimana semata-mata menjadikan internet sebagai bisnis utama (Agus, 2003:2).

Peranan teknologi internet semakin penting, baik untuk kepentingan individu, bisnis, maupun pemerintahan. Dengan adanya internet, dunia seakan tanpa batas (*borderless*), tidak ada lagi hambatan ruang dan waktu dalam menjalin interaksi dengan siapapun dan di manapun. Kita dapat membeli produk dari negara lain melalui internet, melakukan transaksi dalam hitungan detik, mencari informasi dengan memanfaatkan *search engine*, atau

menyelenggarakan pelayanan publik dengan memanfaatkan berbagai aplikasi *e-government*. Di bidang ekonomi, dikembangkan sistem elektronik sebagai infrastruktur untuk kelancaran perdagangan secara elektronik (serambinews, 2014).

Perkembangan jaringan internet tidak hanya memunculkan dampak positif tetapi juga memunculkan dampak negatif, sebagaimana dikemukakan oleh Roy Suryo, seorang pakar teknologi informasi, dalam penelitiannya yang dikutip oleh harian Kompas menyatakan: Kejahatan *cyber crime* kini semakin meningkat karena dilakukan oleh para *hacker* yang rata-rata anak muda yang cukup wawasan dalam kajian ilmu teknologi saat ini, sehingga melibatkan mereka dalam pencurian kartu kredit melalui internet (Roy, 2001:5).

Perbankan adalah lembaga keuangan yang memiliki wewenang untuk menerima deposito atau tabungan dari masyarakat (nasabah) serta mengeluarkan kredit atau pinjaman kepada masyarakat (nasabah). Perkembangan ilmu pengetahuan, informasi dan teknologi, memberikan kemudahan pengembangan sistem perbankan itu sendiri, dengan pengembangan sistem dan layanan untuk memfasilitasi dan memanjakan pelanggannya. Berkenaan dengan fleksibilitas, efisiensi, dan kepraktisan lahirlah sebuah metode baru dalam pengembangan layanan di perbankan bagi pelanggan, di mana sistem ini disebut *electronic banking*, atau biasa dengan istilah *e-banking* yang memungkinkan pengguna layanan pelanggan dapat memanfaatkannya, dimanapun dan

kapanpun, tidak dibatasi oleh waktu dengan layanan. Seiring perkembangan zaman, kebutuhan akan teknologi jaringan komputer pun semakin meningkat. Contohnya sebagai media penyedia informasi, kegiatan komunitas komersial, perbankan, mempermudah transaksi dengan *e-banking* dan *m-banking*. Melalui dunia internet atau *cyber space* dan seiring perkembangannya, menyebabkan munculnya kegiatan *cyber crime* seperti *hacking*, pencurian kartu kredit. (akurat, 2018).

Penerapan teknologi internet perbankan mampu meningkatkan efisiensi dan menurunkan biaya operasional perusahaan. Selain itu, nasabah juga dimudahkan untuk melakukan transaksi *online* dimanapun dan kapanpun. Namun keamanan informasi menjadi isu utama dalam penerapan teknologi internet dalam perbankan, dan pada awal tahun 2018 dunia dikejutkan dengan terjadinya pencurian data melalui mesin ATM di 64 negara dan 13 diantaranya bank swasta dan milik pemerintah Indonesia. Akibat dari kejadian tersebut bank swasta dan bank milik negara mengalami kerugian senilai 18 miliar rupiah (Muhammad, 2018:2). Kejahatan pencurian data ini disebut dengan *cyber crime*.

Cyber Crime ini pernah terjadi di Amerika Serikat yang melibatkan sekitar 200 bank dan Lembaga Keungan yang dilakukan oleh seorang *hacker* asal Aljazair yang bernama Hamza Bendelladj. Dari aksinya itu perbankan dan lembaga keuangan tersebut mengalami kerugian jutaan dollar, meskipun tujuannya tersebut untuk membantu badan amal Palestina. Hamza Bendelladj

menciptakan virus trojan bernama *SpyEye*, dimana virus ini dapat melumpuhkan sistem IT perbankan. Akibat dari aksinya tersebut dia mendapatkan lebih dari 65 tahun hukuman penjara dan harus membayar denda hingga $ 14 juta atau senilai dengan Rp200,455 milliar rupiah (Teknologi, 2016).

BNI Syariah bermula sebagai unit bisnis strategis bagian dari BNI yang mulai beroperasi sejak 29 April 2000. Pada 19 Juni 2010 status BNI Syariah meningkat menjadi Bank Umum Syariah (BUS). Komposisi kepemilikan saham BNI Syariah adalah 99,94% dimiliki oleh PT Bank Negara Indonesia (Persero) Tbk dan sisanya dimiliki oleh PT BNI *Life*. BNI Syariah senantiasa mendapatkan dukungan teknologi informasi dan penggunaan jaringan saluran distribusi infrastruktur BNI Induk diantaranya layanan lebih dari 16.000 ATM BNI, ditambah ribuan jaringan ATM Bersama, ATM Prima serta ATM berlogo *Maestro* dan *Cirrus* di seluruh dunia, fasilitas 24 jam BNI Call (021-1500046), *SMS Banking*, dan BNI *Internet Banking*. Saat ini BNI Syariah telah didukung oleh jaringan yang cukup luas di seluruh Indonesia yaitu 349 *outlet* syariah yang tersebar di seluruh Indonesia, serta didukung oleh lebih dari 1.584 Kantor Cabang BNI yang melayani pembukaan rekening syariah (bnisyariah, 2017).

Dengan adanya dukungan penuh dari bank induk, BNI Syariah sebagai anak perusahaan Bank BNI diperbolehkan untuk memanfaatkan dan mengoptimalkan sistem teknologi informasi yang dimiliki agar dapat tumbuh dan berkembang di tengah

persaingan bisnis yang semakin ketat. Pada tahun 2013, Bank BNI melakukan implementasi internet *banking* yang mengikutsertakan BNI Syariah sehingga internet *banking* yang digunakan sama dengan sistem teknologi informasi Bank Induk. selain itu, Bank BNI juga mengikutsertakan BNI Syariah dalam pengembangan ATM untuk kantor cabang luar negeri sehingga kartu ATM nasabah BNI Syariah dapat digunakan di luar negeri untuk kepentingan pribadi maupun kepentingan bisnis (bnisyariah, 2017)

Bank merupakan sebuah lembaga keuangan yang dipercayakan oleh masyarakat untuk transaksi simpan pinjam. Sedangkan apabila terjadi kehilangan uang tabungan nasabah pada bank tersebut, pihak bank harus bertanggung jawab untuk mengganti uang mereka kembali, Adapun pendapat dari Dosen Perbankan Fakultas Ekonomi dan Bisnis Universitas Malikussaleh Aceh Utara, Marbawi SE MM, menanggapi kasus hilangnya uang tiga nasabah BNI Lhokseumawe. Ia berpendapat, kejadian ini secara langsung telah menurunkan tingkat kepercayaan masyarakat untuk menyimpan uang di BNI. Namun, rasa kurang percaya ini bisa diatasi bila mana pihak bank berani mengumumkan ke publik, apa sebenarnya penyebab uang nasabah tersebut hilang dan bisa memastikan kalau uang yang hilang itu sudah diganti oleh pihak bank.

Marbawi menjelaskan, lazimnya transaksi keuangan bisa dilakukan seorang nasabah menggunakan kartu Anjungan Tunai Mandiri (ATM) dan buku rekening. Sedangkan bila seorang

nasabah tidak melakukan kedua hal ini dan tiba-tiba uangnya hilang, maka sangat besar peluang telah terjadinya *cyber crime* (kejahatan melalui teknologi) yang dilakukan *hacker*. Sedangkan *cyber crime* ini bisa dilakukan dengan metode *skimming*, yakni tindakan pencurian informasi kartu kredit atau debit dengan cara menyalin informasi yang terdapat pada *strip magnetik* kartu kredit atau debit secara ilegal.

Pembobolan rekening nasabah di sejumlah bank dengan sistem *skimming* juga pernah terjadi di Indonesia dan menimpa ratusan nasabah BRI. "Sedangkan ini bisa terjadi, dikarenakan sistem pengawasan di bank tersebut masih lemah. Sudah kewajiban bank selaku lembaga kepercayaan harus terus meningkatkan sistem pengawasannya agar uang di rekening nasabahnya tidak bisa dibobol.

Dalam kasus hilangnya uang tiga nasabah BNI ini, dia juga berpendapat, bila memang benar adanya *cyber crime*, berarti yang melakukan tersebut adalah sindikat internasional. Hal ini sehubungan dengan data yang diperoleh, uang dari rekening salah satu nasabah bisa sampai berpindah ke sebuah rekening di bank Malaysia. Sementara itu, Kapolres Lhokseumawe AKBP Hendri Budiman, melalui Kasat Reskrim AKP Yasir SE, menyebutkan, untuk perkara ini, selain telah diperiksa tiga pelapor, juga telah dimintai keterangan dari penyelia layanan nasabah BNI Cabang Lhokseumawe. Diberitakan sebelumnya, tiga nasabah BNI membuat laporan ke Polres Lhokseumawe atas kehilangan uang

mereka di dalam rekeningnya. Ketiga nasabah tersebut adalah Sri Eka Rizky, warga Hagu Selatan, Kecamatan Banda Sakti, Lhokseumawe. Dia mengetahui uangnya hilang Rp941.642 pada 4 Desember 2016. Lalu, Rosmanita asal Meunasah Masjid, Kecamatan Muara Dua, Lhokseumawe. Dia kehilangan uang Rp22.900.000 pada 10 Januari 2017 malam. Terakhir, Heriansyah warga Meunasah Masjid, Kecamatan Muara Dua, Lhokseumawe. Dia juga kehilangan uang Rp2.766.501 pada 10 Januari 2017 malam (serambinews, 2017)

Berkaitan dengan penanganan pengaduan nasabah, BNI Syariah membentuk unit *Complaint Handling* dan *e-Banking* yang berfungsi untuk menangani pengaduan nasabah akibat tindak kejahatan eksternal, sehingga menciptakan rasa aman dan nyaman dalam melakukan setiap transaksi di BNI Syariah karena ada perlindungan bagi nasabah yang diberikan oleh BNI Syariah (bnisyariah, 2016:186). Tujuan dari penelitian ini yaitu bagaimana mengidentifikasi faktor-faktor yang menyebabkan kejahatan *cyber crime* di Bank BNI Syariah serta bagaimana kebijakan Bank BNI Syariah dalam menangani kejahatan *cyber crime*. Hasil analisis terhadap beberapa penelitian tersebut terdapat beberapa teknik kejahatan *cyber crime* yang sering digunakan, diantaranya yaitu *skimming, hacking* dan *malware*.

Berdasarkan uraian di atas, maka penulis tertarik untuk melakukan penelitian tentang kejahatan *cyber crime*. Untuk itu penulis memilih judul "**Analisis kebijakan Dalam Penanganan**

Kejahatan *Cyber crime* (Studi kasus Bank BNI Syariah Lhokseumawe)".

1.2 Rumusan Masalah

1. Faktor-faktor apa saja yang menyebabkan kejahatan *cyber crime* di Bank BNI Syariah?
2. Bagaimana kebijakan Bank BNI Syariah dalam menangani kejahatan *cyber crime*?

1.3. TujuanPenelitian

1. Untuk mengetahui faktor-faktor yang menyebabkan kejahatan *cyber crime* di Bank BNI Syariah.
2. Untuk mengetahui kebijakan Bank BNI Syariah dalam menangani kejahatan *cyber crime*.

1.4. Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Manfaat Teoritis

Hasil penelitian ini diharapkan dapat menambah pengetahuan bagi mahasiswa Program Studi Perbankan Syariah UIN Ar-Raniry. Penelitian ini juga diharapkan dapat menyumbangkan khasanah kepustakaan dan menambah referensi bagi penelitian selanjutnya.

2. Manfaat Praktik

1. Bagi Perbankan

   Sebagai alternatif dalam antisipasi terhadap kejahatan *cryber crime* yang semakin marak di masa perkembangan teknologi saat ini.

2. Bagi masyarakat

   Hasil penelitian ini diharapkan dapat memberi informasi tentang kejahatan *cyber crime* yang sekarang ini sangat berkembang di dunia teknologi dan internet.

1.5 Sistematika Pembahasan

Hasil penelitian ini akan disusun dalam bentuk skripsi dengan sistematika penulisan sebagai berikut:

BAB I Pendahuluan

Bab pendahuluan ini berisi tentang latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian dan sistematika pembahasan

BAB II Landasan teori

Bab landasan teori ini berisi tentang kerangka teori, temuan penelitian terkait, model penelitian atau kerangka pemikiran.

BAB III Metode Penelitian

Bab metode penelitian ini berisi tentang jenis penelitian, data dan teknik pemerolehan data, dan teknik pengumpulan data.

BAB IV Hasil Penelitian dan Pembahasan

Bab hasil penelitian dan pembahasan ini memuat deskripsi penelitian objek penelitian, hasil analisis serta pembahasan secara mandalam tentang hasil temuan dan menjelaskan implikasinya.

BAB V Penutup

Bab ini merupakan penutupan dari pembahasan skripsi yang memuat kesimpulan dan saran atau rekomendasi.

BAB II

LANDASAN TEORI

2.1 Kerangka Teori

2.1.1 Kejahatan *Cyber Crime*

Cyber crime adalah suatu aktivitas kejahatan di dunia maya dengan memanfaatkan jaringan komputer sebagai alat dan jaringan internet sebagai medianya.

1. Dalam arti luas, pengertian *cyber crime* adalah semua tindakan ilegal yang dilakukan melalui jaringan komputer dan internet untuk mendapatkan keuntungan dengan merugikan pihak lain.
2. Dalam arti sempit, pengertian *cyber crime* adalah semua tindakan ilegal yang ditujukan untuk menyerang sistem keamanan komputer dan data yang diproses oleh suatu sistem komputer (Maxmanroe, 2018).

Berikut ini beberapa pengertian *cyber crime* dari beberapa sumber buku:

1. Menurut Wahid dan Labib (2010:40), *cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.
2. Menurut Widodo (2011:7), *cyber crime* adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sasaran

kejahatan. Semua kejahatan tersebut adalah bentuk-bentuk perbuatan yang bertentangan dengan peraturan perundang-undangan, baik dalam arti melawan hukum secara materiel maupun melawan hukum secara formal.

3. Menurut Parker (Hamzah, 1993:18), *cyber crime* adalah suatu kejadian yang berhubungan dengan teknologi komputer yang seorang korban menderita atau akan telah menderita kerugian dan seorang pelaku dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan.
4. Menurut *Organization of European Community Development* (OECD), *cyber crime* atau kejahatan komputer adalah segala akses ilegal atau akses secara tidak sah terhadap suatu transmisi data sehingga telihat bahwa segala aktivitas yang tidak sah dalam suatu sistem komputer merupakan suatu kejahatan (Karnasudirja, 1993:3).

2.1.2 Sejarah Bermula Terjadinya *Cyber Crime*

Sejarah awal bermula terjadinya kejahatan *cyber crime* sudah dilakukan penelitian oleh *Stenford Research International* (SRI) di Amerika Serikat sejak 1971 sampai tahun 1985. Penelitian tersebut menemukan 1600 kasus yang terjadi sejak tahun 1958, serta reaksi masyarakat dan pemerintah terhadapnya, termasuk penyelesaian berdasarkan hukum perdata. Dalam tahun 1979 SRI mendapatkan data yang

lebih valid, yaitu menyatakan bahwa dari 244 kasus yang terjadi, ada 191 yang dapat diajukan ke pengadilan dan terdakwa dari 161 kasus dapat dipidana. Penelitian- penelitian yang dilakukan pada tahun 1970-an tersebut belum dapat menunjukkan data secara jelas pengaturanya dalam hukum pidana sehingga belum dimasukan ke dalam statistik kriminal. Penelitian lainnya dilakukan di Jerman, Australia, Inggris, Swedia, Finlandia, Austria, Jepang, Kanada dan Belanda. Semua penelitian tersebut bahwa *cyber crime* selalu meningkat dari tahun ke tahun.

Beberapa bentuk *cyber crime* di Amerika Serikat yang menarik perhatian masyarakat antara tahun 1974 sampai tahun 1988 adalah sebagai berikut.

1. Tahun 1974 sejumlah mahasiswa *Brooklyn Collage New York* secara tidak sah mengakses data pada komputer di bagian registrasi akademik, kemudian mengubah data pada daftar prestasi akademik milik mereka sendiri dan teman-temanya secara *online*. Setelah diadakan investigasi perbuatan tersebut terbukti diakukan oleh 12 mahasiswa.
2. Tahun 1977 dua orang karyawan bagian pemograman komputer dalam suatu perusahaan menggunakan komputer perusahaan tersebut secara tidak sah selama 3 tahun. Komputer tersebut digunakan untuk memenuhi kebutuhan perusahaan lainya yang didirikan oleh pelaku kejahatan,

3. Tahun 1986 tiga orang anak ditahan oleh kepolisian Amerika Serikat karena diduga kuat menghancurkan sistem keamanan TRW perusahaan kartu kredit dan mengopy nomor kartu kredit orang lain kemudian membelanjakan USD 10.000.
4. Tahun 1988 seorang mahasiswa berhasil memasukan virus *internet worm* dalam sistem internet yang mengakibatkan gangguan terhadap 6000 sistem internet (Karnasudirja. 1999:20).

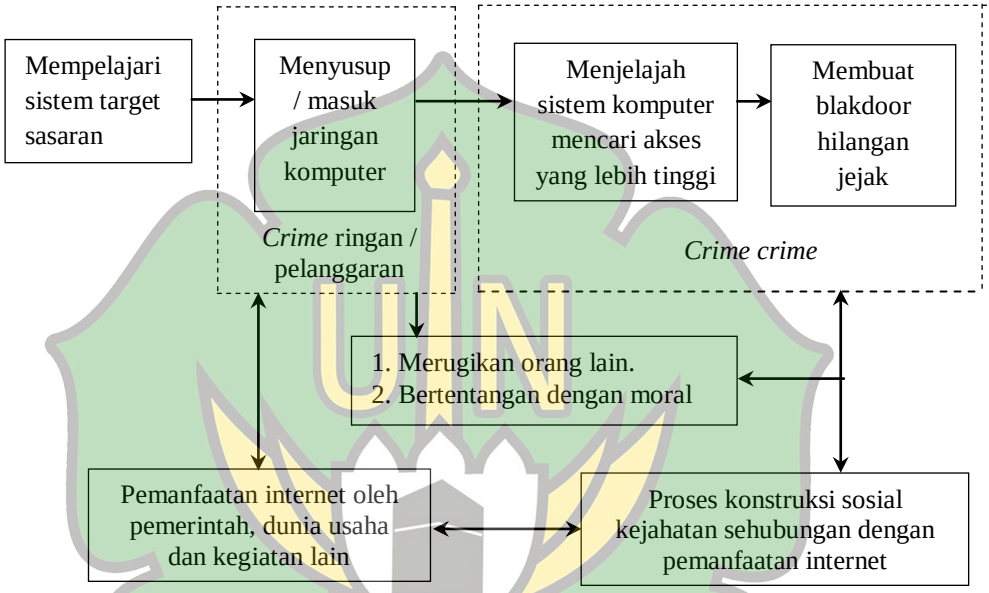
2.1.3 Karakteristik *Cyber Crime*

Menurut Wahid dan Labib (2010:76), kejahatan dunia maya atau *cyber crime* memiliki beberapa karakteristik, yaitu sebagai berikut:

1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah *cyber* (*cyber space*), sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apa pun yang terhubung dengan internet.
3. Perbuatan tersebut mengakibatkan kerugian materiel maupun imateriel (waktu, nilai, jasa, uang, barang, harga diri, martabat dan kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.

5. Perbuatan tersebut sering dilakukan secara transaksional/melintas batas negara.

Skema dan gambar proses pelaksanaan *cyber crime* ditunjukkan pada gambar di bawah ini :



Sumber : (Raharjo, 2002:199)

Gambar 1.1

Skema dan Proses *cyber crime*

Adapun langkah-langkah yang biasa dilakukan dalam aktivitas *cyber crime* menurut gambar di atas ialah: (Raharjo, 2002:199):

1. Mengumpulkan dan mempelajari informasi yang ada mengenai sistem operasi komputer atau jaringan komputer yang dipakai pada target sasaran.

2. Menyusup atau mengakses jaringan komputer target sasaran.
3. Menjelajahi sistem komputer dan mencari akses yang lebih tinggi.
4. Membuat *backdoor* dan menghilangkan jejak.

2.1.4 Karakteristik *Cyber Crime* di Indonesia

Berdasarkan hasil penelitian Widodo, motivasi pelaku *cyber crime* di Indonesia adalah mencoba kemampuan dan keterampilan diri sendiri dalam mengoperasikan peralatan teknologi informasi menguji pihak lain yang mengelola dan mengamankan *situs/website*, bersenang-senang ingin dianggap sebagai pahlawan (hero) memperkenalkan atau mempopulerkan kelompok *hecker/cracker*, memperoleh uang, balas dendam, politik pelampiasan kekecewaan, dan persaingan usaha. Dalam satu bentuk kejahatan kemungkinan di dorong oleh lebih dari satu motivasi. Antara satu bentuk kejahatan dengan kejahatan lainya, mempunyai motivasi yang berbeda. Karena itu teori kriminologi tentang *Multipile Factor Theory* dapat digunakan sebagai pisau analisis penyebab pelaku *cyber crime* di Indonesia (Widodo, 2006).

Karakteristik *cyber crime* di Indonesia adalah sebagai berikut (Widodo, 2006):

1. Bersifat lintas Negara (*Trans-National Crime*).
2. Bukan hanya menggunakan komputer konvensional (melainkan sudah menggunakan laptop, hanphone dan tablet).
3. Ada yang dapat digolongkan sebagai *white collar criminal* dan ada yang bukan *white collar criminal.*
4. Bukan merupakan kejahatan organisasi.
5. Dapat berupa kejahatan korporasi dan bukan kejahatan korporasi.

Sedangkan karakteristik pelaku *cyber crime* di Indonesia adalah sebagai berikut (Widodo, 2006):

1. Mempunyai keterampilan yang sangat memadai dalam mengoperasikan komputer, internet, serta program aplikasinya.
2. Berpendidikan relatif tinggi (termasuk mahasiswa).
3. Tinggal di kota-kota besar yaitu ibu kota kabupaten, provinsi, dan negara.
4. Menyukai tantangan di bidang teknologi informasi yang berbasis komputer.
5. Mayoritas berjenis kelamin laki-laki.
6. Mempunyai kreativitas yang tinggi dan teliti.

7. Pandai memanfaatkan peluang yang ada untuk melakukan kejahatan dan mayoritas tergabung dalam komunitas *underground*.

Berkaitan dengan hasil penelitian Widodo, juga berdasarkan pendapat *Sue Titus Reid*, secara umum ternyata *cyber crime* diluar Indonesia dapat dilakukan secara organisasi (*organized crime*) dan dapat dilakukan oleh orang-orang terhormat dengan cara menyalahgunakan wewenangnya (*white collar crime*). Saat ini bahkan *cyber crime* memiliki karakteristik yang semakin unik, karena pengguna *cyber space* sudah membentuk masyarakat tersendiri, yang lazim disebut *underground*. Lewat komunitas inilah para pengguna internet dapat saling berkomunikasi, berinteraksi di dunia maya, bahkan saling memberikan informasi yang mungkin dapat mengarah pada perbuatan jahat.

Meskipun pelaku kejahatan tersebut saling terikat dengan komunitas *underground*, tetapi keterkaitan tersebut hanya sebatas komunikasi dan tukar menukar informasi melalui internet (*chatting*) sehingga tidak ada hubungan struktural dan fungsional sebagaimana ada dalam setiap organisasi formal. Menurut Agus Rahardjo dalam *cyber space* terdapat *whole world lectronic link* (WELL) yaitu sebuah tempat yang memungkinkan orang-orang dari seluruh dunia saling berbicara atau bercakap-cakap untuk bertukar informasi.

2.1.5 Bentuk-Bentuk Kejahatan *Cyber Crime*

Secara umum, Ari Juliano Gema mengemukakan *cyber crime* dapat di kelompokkan dalam bentuk sebagai berikut:

1. *Anuthorized access to computer system and service*

   Kejahatan ini dilakukan dengan cara memasuki atau menyusup secara tidak sah kedalam suatu sistem atau jaringan komputer. Tujuan dari perbuatan tersebut adalah sabotase atau pencurian data atau pemalsuan informasi penting dan rahasia. Ciri utama dari perbuatan ini adalah memasuki sistem secara tidak sah.

2. *Ilegal Contents*

   Kejahatan ini dilakukan dengan jalan memasukkan data atau informasi ke dalam jaringan internet tentang semua hal yang tidak benar, tidak etis dan dapat melanggar hukum atau ketertiban umum. Perbuatan tersebut misalnya pemuatan berita bohong, fitnah, pornografi, pembocoran rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah. Unsur utama pada kejahatan ini adalah pada "isi" data yang dimasukan ke dalam jaringan komputer.

3. Data *Forgery*

   Kejahatan ini dilakukan dengan cara memalsu data pada dokumen-dokumen penting yang tersimpan dalam sistem komputer sebagai *scriptless* dokumen melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen perdagangan elektronik (*ecommerce*) dengan cara membuat

pesan seolah-olah terjadi kesalahan pengetikan yang dapat menguntungkan pelaku, karena korban sudah terlanjur memasukkan data pribadi dan PIN kartu kredit sehingga pelaku memungkinkan menyalahgunakan data tersebut.

4. *Cyber Espionage*

Kejahatan ini dilakukan dengan jalan memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata (*spionase*) terhadap pihak lain dengan cara memasuki sistem jaringan komputer (*computer network system*) pihak lain. Kejahatan ini biasanya ditujukan kepada orang atau saingan perusahaan bisnis yang dokumen atau data rahasia (*data base*) tersimpan dalam suatu sistem komputer yang tersambung ke jaringan komputer.

5. *Cyber Sabotage and Extortion*

Kejahatan ini dilakukan dengan cara membuat gangguan, perusakan atau penghancuran terhadap data, program atau sistem jaringan komputer yang terhubung dengan internet secara tidak sah. Kejahatan ini dilakukan dengan cara menyusupkan suatu *logic bomb*, virus komputer atau suatu program tertentu, sehingga data program atau sistem jaringan komputer tidak dapat digunakan, tidak dapat beroperasi sebagaimana mestinya, atau dapat beroperasi tetapi tidak sesuai dengan kehendak pelaku kejahatan.

6. *Offense Against Intellectual Property*

Kejahatan jenis ini ditunjukan terhadap Hak Kekayaan Intelektual (HAKI) yang dimiliki oleh pihak lain di internet sebagai contoh adalah penjiplakan tampilan pada *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang merupakan rahasia dagang milik pihak lain.

7. *Infrigments Of Privacy*

Kejahatan jenis ini ditunjukan terhadap data atau informasi seseorang yang bersifat individual dan rahasia (*privacy*) secara melawan hukum. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada data formulir pribadi yang tersimpan secara *computerized*. Jika data tersebut diketahui oleh orang lain, dapat merugikan pemilik informasi baik secara materiel maupun immateriel misalnya nomor kartu kredit, PIN, ATM, catatan-catatan pribadi, cacat tubuh, atau penyakit-penyakit tersembunyi (gema, 2013)

Selain penggolongan *cyber crime* Donn Parker mengklarifikasikan bentuk-bentuk *cyber crime* ke dalam 4 (empat) klarifikasi berikut:

1. Komputer sebagai objek dalam kategori ini, bentuk-bentuk *cyber crime* kasus-kasus perusakan terhadap komputer, data atau program yang terdapat di dalamnya atau perusakan terhadap sarana-sarana komputer seperti *Air Conditioning*

(AC) dan peralatan listrik yang menunjang pengoperasian komputer.

2. Komputer sebagai subjek komputer dapat pula menimbulkan tempat atau lingkungan untuk melakukan kejahatan, misalnya penipuan, pencurian dan pemalsuan yang menyangkut harta benda dalam bentuk baru yang tidak dapat disentuh (*intangible*), misalnya pulsa elektronik dan guratan-guratan pita magnetis.
3. Komputer digunakan sebagai alat kejahatan sehingga peristiwa kejahatan tersebut adalah sangat kompleks dan sulit diketahui. Salah satu contoh seseorang pelaku kejahatan yang mengambil warkat-warkat setoran dan menulis nomer rekening pelaku dengan tinta magnetis pada warkat tersebut, kemudian meletakkan kembali di tempat semula. Nasabah yang akan memasukkan uang akan mengambil dan mengisi warkat yang sudah dibubuhi nomer rekening pelaku kejahatan tersebut sebagai bukti penyetoran. Pada waktu komputer memproses warkat-warkat nasabah, komputer secara otomatis akan mengkredit sejumlah uang pada rekening pelaku kejahatan, setelah itu pelaku kejahatan akan menarik uang dengan cek dari rekening sebelum para nasabah yang menyetor mengajukan komplain terhadap pihak bank.
4. Komputer sebagai simbol dapat digunakan sebagai simbol untuk melakukan penipuan atau ancaman.

J. Sudama Sastraandaja juga menyatakan bahwa *cyber crime* dapat dikalsifikasikan dalam 5 bentuk sebagai berikut:

1. Kejahatan-kejahatan yang menyangkut data atau informasi komputer.
2. Kejahatan-kejahatan yang menyangkut program atau software komputer.
3. Pemakaian fasilitas-fasilitas komputer tanpa wewenang untuk kepentingan yang tidak sesuai dengan tujuan atau pengelolaan pengoperasianya.
4. Tindakan-tindakan yang mengganggu operasional komputer.
5. Tindakan perusakan terhadap peralatan komputer atau peralatan-peralatan yang berhubungan dengan komputer atau sarana-sarana penunjangnya (Deris, 2005).

Andi Hamzah menguraikan bahwa bentuk-bentuk kejahatan *cyber crime* di atas dapat dikaitkan dengan ketentuan-ketentuan dalam buku II KUHP Indonesia. Jika dibuat perbandingan maka akan diperoleh deskripsi sebagaimana uraian berikut.

1. Joy Computing

Adalah perbuatan seseorang yang menggunakan komputer secara tidak sah atau tanpa izin dari pihak yang berwenang dan penggunaannya melampaui kewenangan yang dimiliki. Tindakan ini dapat dikategorkan sebagai tindakan pidana pencurian (Pasal 362 KUHP).

2. Hacking

Adalah perbuatan berupa penyambungan saluran, yaitu dengan cara menambah terminal komputer baru pada sistem jaringan komputer tanpa izin (dilakukan dengan melawan hukum) dari pemilik sah jaringan komputer. Tindakan ini dapat dikategorikan sebagai tindakan pidana, yaitu tindakan yang masuk tanpa wewenang masuk dengan memaksa ke dalam rumah atau ruang yang tertutup atau pekarangan atau tanpa haknya berjalan di atas tanah milik orang lain (pasal 167 dan pasal 551 KUHP)

3. *The Trojan Horse*

Adalah menambah, mengurangi atau mengubah instruksi pada sebuah program sehingga program tersebut selain menjalankan tugas yang semestinya juga akan melaksanakan tugas lain yang tidak sah sebagaimana yang dikehendaki pelaku kejahatan tindakan ini dikategorikan sebagai tindakan pidana penggelapan (pasal 372 dan pasal 374 KUHP). Apa bila kerugian yang ditimbulkan menyangkut keuangan Negara, tindakan tersebut dapat dikatagorikan dalam tindak pidana korupsi.

4. Data *Leakgage*

Adalah tindakan pembocoran data rahasia yang diakukan dengan cara menulis data rahasia tersebut ke dalam kode-kode tertentu sehingga data dapat dibawa keluar sistem komputer tanpa diketahui oleh pihak yang bertanggung jawab terhadap

data tersebut. Tindakan ini dapat dikategorikan sebagai tindak pidana terhadap keamanan Negara (pasal 112, 113,114, dan pasal 115 KUHP) dan tindak pidana membuka rahasia perusahaan atau kewajiban menyimpan rahasia profesi atau jabatan (pasal 332 dan pasal 323 KUHP).

5. Data *Diddiling*

Adalah suatu tindakan pelanggaran hukum yang mengubah validitas data. Perbuatan ini dilakukan dengan cara mengubah input atau output data. Tindakan ini dapat dikategorikan sebagai tindak pidana pemalsuan surat (Pasal 263 KUHP).

6. Penyia-nyian Data Komputer

Penyia-nyian Data Komputer dapat diartikan sebagai suatu perbuatan yang dilakukan dengan sengaja untuk merusak atau menghancurkan media disket dan media penyimpanan sejenis lainya misalnya hardisc. Yang berisi data atau program komputer sehingga data atau program tersebut tidak berfungsi sebagaimana mestinya. Tindakan ini dapat dikategorikan sebagai tindak pidana perusakan barang Pasal 406 KUHP (Adi, 1996:279).

2.1.6 Jenis-Jenis *Cyber Crime*

Terdapat beberapa jenis kejahatan *cyber crime* yang sering terjadi sebagaimana yang dikutip dari berbagai sumber tepercaya, antara lain sebagai berikut:

1. *Unauthorized Aces*

   Kriminal yang berlangsung apabila seorang memasuki atau menyusup ke dalam sesuatu skema jaringan komputer dengan cara tidak legal, tanpa izin, atau tanpa sepengetahuan dari pemilik skema jaringan komputer yang dimasukinya.

2. *Illegal Contents*

   Kriminal yang dijalani dengan metode memuatkan informasi atau informasi ke internet berhubungan sesuatu keadaan yang tidak benar, tidak sopan, serta bisa diduga sebagai melanggar hukum atau mengganggu ketertiban pada publik umum,

3. Penyebaran Virus Secara Sengaja

   Penyebaran virus pada umumnya dilakukan dengan menggunakan sebuah email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.

4. *Cyber Espionage, Sabotage* dan *Extortion*

   Cyber Espionage merupakan sebuah kejahatan dengan cara memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. *Sabotage and Extortion* merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

5. *Carding*

Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

6. *Hacking dan Cracker*

Istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Aktivitas *cracking* di internet memiliki lingkup yang sangat luas, mulai dari pembajakan *account* milik orang lain, pembajakan situs web, *probing*, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (*Denial Of Service*). *Dos attack* merupakan serangan yang bertujuan melumpuhkan target (*hang, crash*) sehingga tidak dapat memberikan layanan.

7. *Cybersquatting And Typosquatting*

Cybersquatting merupakan sebuah kejahatan yang dilakukan dengan cara mendaftarkan *domain* nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun *typosquatting* adalah kejahatan dengan membuat *domain plesetan* yaitu *domain* yang mirip dengan nama *domain* orang lain.

8. *Cyber Terorism*

Suatu bentuk kegiatan terencana yang termotivasi secara politis yang berupa serangan terhadap informasi, sistem komputer, program komputer dan data sehingga mengancam pemerintah atau warganegara, termasuk *cracking* ke situs pemerintah atau militer (Abidin, 2015).

2.1.7 Kejahatan *Cyber Crime* Dalam Dunia Perbankan

Dari beberapa macam *cyber crime* yang terjadi, Indonesia salah satu *cyber crime* yang marak terjadi yaitu kejahatan *carding* (kartu kredit), kejahatan ini lebih dikhususkan dalam transaksi penjualan baik itu yang dilakukan secara *online* maupun secara fisik. Secara fisik, *carding* dilakukan dengan mengunakan kartu kredit milik orang lain untuk berbelanja di tempat belanja yang menerima pembayaran memakai kartu kredit. Baik di tempat pembelanjaan yang modern, mall, toko mas, serta semua tempat-tempat yang berlogo *Master, Visa, Maestro, Cirrus, American-Express* dan sebagainya. Teknik penggandaan kartu kredit dilakukan dengan membaca data kartu kredit mengunakan MSR (*Magnetic StripeCard Reader*), lalu datanya ditulis ke sebuah kartu kosongan atau kartu bodong menggunakan *Magnetic StripeCard Writer*. Selanjutnya kartu inilah yang digunakan untuk berbelanja secara phisical ke berbagai tempat yang melayani pembayaran dengan kartu kredit. Sementara itu, secara *online*, *carding* dilakukan dengan menggunakan kartu kredit milik orang lain atau

nomor kartu kredit milik orang lain untuk berbelanja di tempat belanja *online*. Selain itu, tentang teknik *hacking* kartu kredit alias *carding*, yakni melakukan pencurian data transaksi dari pengelola suatu layanan *online* shopping yang dilakukan oleh seorang *black hacker*. Selanjutnya data pemilik kartu kredit dari database ini si *hacker/cracker* (sebutan untuk mereka yang masuk ke sistem orang lain) mengunakannya untuk bertransaksi dan otomatis tagihannya akan masuk kepada pemilik kartu kredit (Arief, 2006:13).

Ada beberapa cara yang digunakan hacker untuk mencuri kartu kredit antara lain sebagai berikut:

1. Paket *Snifer*

   Sniffing adalah tindakan untuk mendapatkan data dengan memasukkan program paket *sniffer* untuk mendapatkan *account name* dan *password* yang akan digunakan. Menurut *The Computer Emergency Response Team Coordination Center* (*CERT CC*), paket *sniffing* adalah salah satu insiden yang paling banyak terjadi. Pada umumnya yang diincar adalah website yang tidak dilengkapi *security encryption* atau situs yang tidak memiliki keamanan yang bagus.

2. Membuat Program *Spyware, Trojan, Worm*

   Spyware, trojan, worm dan sebagainya digunakan sebagai *keylogger* (*keyboard logger*, program mencatat aktivitas *keyboard*) dan program ini disebar lewat e-mail *spamming* dengan meletakkan file-nya di *attachment, mirc* atau fasilitas chatting lainnya, atau situs-situs tertentu dengan icon atau

iming-iming yang menarik *netter* (seseorang yang menggunakan/menjelajah internet untuk mencari suatu informasi) untuk men-download dan membuka file tersebut.

3. Membuat situs Phising

Phising digunakan untuk memancing pengguna internet mengunjungi sebuah situs tertentu. Dalam hal pencurian *account credit card*, pelaku membuat situs dengan nama yang hampir sama dengan situs aslinya. Contohnya, situs klik btc www. Klikbtc.com, dibuat dengan nama yang mirip yaitu www.clickbtc.com atau www.kikbtc.com. Hal ini memungkinkan untuk mengambil keuntungan dari kemungkinan salah ketik yang dilakukan oleh netter. Namun, pelaku dari pembuatan situs tersebut mengaku tidak berniat jahat.

4. Membobol situs e-commerce

Cara ini agak sulit dan perlu pakar *cracker* (sebutan untuk mereka yang masuk ke sistem orang lain) atau *cracker* yang sudah pengalaman untuk melakukannya. Pada umumnya mereka memakai metode *injection* (memasukkan *script* yang dapat dijalankan oleh situs/server) bagi situs yang memiliki *firewall*. Menyadari bahwa *carding* sebagai salah satu jenis *cyber crime* sudah termasuk kejahatan yang meresahkan, apalagi mengingat Indonesia dikenal sebagai surga bagi para *carder* (pelaku kejahatan *carding*), maka Polri menyikapinya dengan membentuk suatu satuan khusus di tingkat Mabes Polri

yang dinamakan Direktorat *cyber crime* yang ditempati oleh personil terlatih untuk menangani kasus-kasus semacam ini, tidak hanya dalam teknik penyelidikan dan penyidikan, tapi juga mereka menguasai teknik khusus untuk pengamanan dan penyitaan bukti-bukti secara elektronik. Akan tetapi kemampuan hukum untuk menanggulangi kejahatan mengalami penurunan, hal ini dikarenakan struktur hukum dengan fungsi hukum tidak berkembang secara paralel sehinga penegakan hukum cenderung terus melemah (Mahfud M.D, 2000 : 35).

2.2 Penelitian Terkait

Penelitian yang terkait sebelumnya merupakan hal yang sangat bermanfaat untuk menjadi perbandingan dan acuan yang memberikan gambaran terhadap hasil-hasil penelitian terdahulu menyangkut kejahatan *cyber crime*. Untuk melakukan penelitian diperlukan hasil penelitian sebelumnya agar dapat di jadikan referensi perbandingan dalam penelitian.

Berikut ini beberapa penjelasan penelitian sebelumnya di antaranya:

Tabel 2.1 Penelitian Terkait

No	Nama Peneliti	Judul Penelitian	Metode Penelitian	Hasil Penelitian
1.	Harry (2015)	Perlindungan Hukum Terhadap Nasabah Bank Pengguna Fasilitas Internet	Yuridis Sosiologis	Perlindungan hukum atas data pribadi dan dana nasabah dalam penyelenggaraan internet banking dengan pendekatan

Tabel 2.1 – Lanjutan

No	Nama Peneliti	Judul Penelitian	Metode Penelitian	Hasil Penelitian
		Banking atas Terjadinya *Cyber Crime* (Studi Kasus: Bussines *Banking Center* Mandiri Padang		pengaturan secara internal dari penyelenggara internet banking itu sendiri.
2.	Kian (2015)	Tindak Pidana *Credit/Debit Card Fraud* dan Penerapan Sanksi Pidananya dalam Hukum Pidana Indonesia	Penelitian Normatif	Pengaturan dan sanksi pidana terhadap tindak pidana *credit/debit card fraud* di Indonesia masih tergolong minim.
3.	Rahmah (2018)	Pengaruh Penggunaan Internet Banking Dan Perlindungan Nasabah Pengguna Fasilitas Internet Banking Terhadap *Cyber Crime* Di Daerah Istimewa Yogyakarta (Diy)	Pendekatan Kuantitatif	Semakin banyak nasabah yang memanfaatkan fasilitas internet banking dapat memicu terjadinya cyber crime. Mengingat era sekarang ini sudah memasuki era digital, sehingga semakin banyak orang yang terampil dalam menggunakan teknologi dan tidak sedikit dari mereka yang justru menyalahgunakan teknologi tersebut.
4.	Silalahi (2012)	Analisis Yuridis Kejahatan *Cyber Crime* Dalam Pembobolan Mesin ATM Bank	Metode Kualitatif	Pembobolan ATM bank yang dilakukan oleh pelaku dapat dihukum dalam hukum pidana atau dalam KUHP serta dapat dijerat dengan

Tabel 2.1 – Lanjutan

No	Nama Peneliti	Judul Penelitian	Metode Penelitian	Hasil Penelitian
				Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronika. Sedangkan bagi nasabah / korban pembobolan ATM bank pihak bank selaku pelaku pemberi jasa dapat mengganti kerugian dari nasabah korban pembobolan ATM bank.

Sumber: Data diolah (2019)

Dari tabel 2.1 terdapat persamaan dan perbedaan penelitiannya dengan penelitian penulis. Penelitian yang telah ada sebelumnya dan sesuai dengan penelitian ini adalah sebagai berikut:

Penelitian yang dilakukan oleh Nidia Putri Harry (2015) terdapat persamaan yaitu sama-sama mengkaji tentang kejahatan *cyber crime* yang menyerang nasabah. Sedangkan perbedaan dalam penelitian ini yaitu teknik pengambilan datanya. Dalam penelitian ini menggunakan metode pendekatan yuridis sosiologis, hukum sebagai *law in action*, dideskripsikan sebagai gejala sosial yang empiris. Sedangkan penulis menggunakan metode deskriptif analisis dengan cara mendeskripsikan faktor-faktor yang menyebabkan kejahatan *cyber crime*.

Penelitian yang dilakukan oleh Antonius Maria Laot Kian (2015) terdapat persamaan yaitu sama-sama mengkaji tentang kejahatan *cyber crime*. Sedangkan perbedaan dalam penelitian ini yaitu teknik pengambilan datanya. Dalam penelitian ini menggunakan tipe penelitian hukum normatif. Penelitian ini berpijak pada konstruksi norma hukum positif. Sedangkan penulis berpijak pada penerapan penggunaan internet *banking* dalam konteks kejahatan *cyber crime* yang menyerang nasabah.

Penelitian yang dilakukan oleh Yuslia Naili Rahmah (2018) terdapat persamaan yaitu sama-sama mengkaji tentang kejahatan *cyber crime*. Sedangkan perbedaan dalam penelitian ini yaitu penelitian yang dilakukan lebih menfokuskan pada bagian data untuk perlindungan terhadap nasabah yang memanfaatkan *internet banking* sehingga dapat memicu terjadinya *cyber crime.* Sedangkan penulis menfokuskan terhadap kejahatan secara ekternal seperti *trapping, skimming, pharming, phising* dan ancaman *cyber crime*.

Penelitian yang dilakukan oleh Hatialum Rehulina Br Silalahi (2012) terdapat Persamaan yaitu sama-sama mengkaji tentang kejahatan *cyber crime* yang menyerang nasabah. Sedangkan perbedaan dalam penelitian ini yaitu teknik pengambilan datanya. Dalam penelitian ini menggunakan metode kualitatif dengan menggunakan angket atau kuesioner. Sedangkan penulis menggunakan metode kualitatif dengan menggunakan wawancara langsung saja tanpa angket atau kuesioner. Selain itu juga dalam penelitian ini yang dikaji hanya kasus pembobolan ATM saja

sedangkan penelitian yang akan saya lakukan lebih terfokus pada kejahatan *cyber crime* di semua produk *internet banking*.

2.3 Kerangka Berpikir

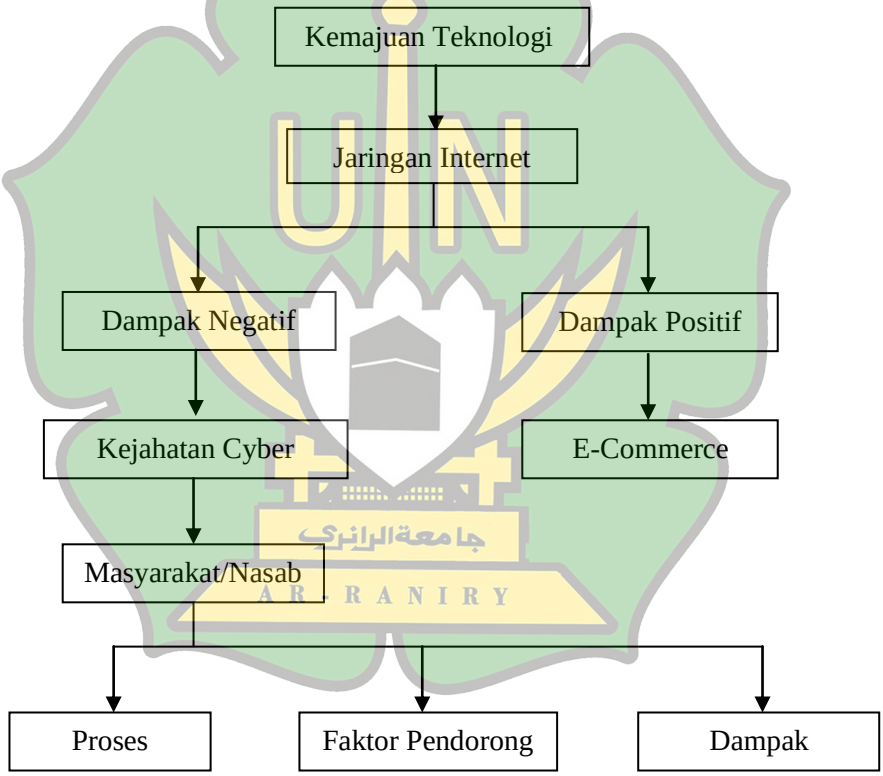
Dalam penelitian ini dikembangkan suatu konsep atau kerangka berpikir dengan tujuan untuk mempermudah peneliti dalam melakukan penelitian. Dengan adanya kerangka pikir ini maka tujuan yang akan dicapai oleh peneliti dalam penelitian akan lebih terarah karena telah terkonsep secara jelas.

Kerangka pikir yang menjadi garis besar dalam penelitian ini adalah kejahatan *Cyber crime*. Beberapa tahun terkahir perkembangan teknologi komunikasi dan informasi berkembang dengan pesat, hampir dalam segala bidang terjamah akan perkembangan teknologi tersebut. Munculnya berbagai penemuan baru memberikan kemudahan dalam kehiduapan manusia, khususnya dalam bidang komunikasi dengan diketemukanya internet yang memberikan dampak yang cukup besar.

Dengan adanya internet bukan hanya memberikan manfaat terhadap kehidupan manusia, namun juga memunculkan dampak negatif yang tidak dapat dihindari. Salah satu dampak negatif yang muncul dari adanya internet adalah kejahatan *Cyber crime*.

Masyarakat atau nasabah sebagai salah satu pengguna internet aktif, juga ikut terpengaruh dari adanya dampak negatif internet tersebut. Dampak negatif dari adanya internet yang berpengaruh terhadap masyarakat ditunjukan dengan adanya keterlibatan masyarakat dalam kejahatan *Cyber crime*.

Berdasarkan keadaan tersebut, peneliti tertarik untuk melakukan penelitian tentang bagaimana proses masyarakat atau nasabah mengenal kejahatan *Cyber crime*, faktor pendorong yang menyebabkan mereka terlibat dalam kasus kejahatan *Cyber crime*, serta dampak yang dirasakan setelah keterlibatan mereka dalam kejahatan *Cyber crime*.



Sumber : (Arief, 2006)

Gambar 2.1 Kerangka Berpikir

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian ini merupakan penelitian kualitatif yang menggunakan metode deskriptif analisis. Apabila seseorang melakukan penelitian yang terbatas, tetapi dengan keterbatasan sasaran penelitian yang ada itu digali sebanyak mungkin data mengenai sasaran penelitian. Semakin berkualitas data yang dikumpulkan, maka penelitian ini semakin berkualitas (Bungin, 2013:29). Oleh karena itu, dalam hal ini penulis menggunakan cara mendeskripsikan faktor-faktor yang menyebabkan kejahatan *cyber crime* di Bank BNI Syariah melalui analisis penerapan penggunaan internet *banking* dalam konteks kejahatan *cyber crime* yang menyerang nasabah.

Menurut Ghony dan Almashur (2012:25) penelitian kualitatif adalah penelitian yang menghasilkan penemuan-penemuan yang tidak dapat dicapai dengan menggunakan prosedur statistik atau dengan cara-cara kuantifikasi. Sedangkan metode deskriptif analitis adalah penelitian yang menggambarkan data-data informasi berdasarkan fakta yang diperoleh dilapangan (Danim, 2002). Adapun tujuan dari menganalisis kedua hal ini adalah untuk membuat deskripsi antara objek dengan fakta yang ada agar nasabah mendapatkan informasi yang jelas ketika menggunakan internet *banking*.

3.2 Jenis Data dan Sumber Data

Dalam skripsi ini, penulis menggunakan dua jenis sumber data, yaitu:

a. Data primer

Data primer adalah data yang diperoleh langsung dari sumber data pertama di lokasi penelitian atau objek penelitian (Bungin, 2001: 129). Dalam penelitian ini, data yang diperoleh langsung yaitu data dari hasil wawancara kepada pihak Bank BNI Syariah dan Kapolres Lhokseumawe, yaitu hasil pertanyaan terkait dengan penelitian. Data primer di dapat dari sumber informan yaitu individu atau perseorangan seperti hasil wawancara yang dilakukan oleh peneliti.

b. Data Sekunder

Data sekunder adalah data yang diperoleh dari sumber kedua atau sumber sekunder yang kita butuhkan (Bungin, 2001: 129). Dalam penelitian ini, data yang dibutuhkan berupa literatur-literatur kepustakaan seperti buku-buku, artikel, surat kabar, internet, dan kasus-kasus kejahatan *cyber crime* yang menyerang nasabah serta sumber lainnya yang berkaitan dengan materi penulisan skripsi ini.

3.3 Teknik Pengumpulan Data

Sesuai dengan permasalahan yang diangkat di atas, maka dalam pengumpulan data skripsi ini, penulis menggunakan metode pengumpulan data sebagai berikut:

a. Penelitian lapangan (*field research*) yaitu data yang dibutuhkan dalam penelitian ini adalah jenis primer, yaitu data yang didapatkan dari lapangan atau pengumpulan data dengan melakukan interview kepada pihak-pihak yang memberikan informasi untuk penelitian ini. Dengan metode ini penulis memperoleh data dan informasi tentang kejahatan *cyber crime* dengan menggunakan teknik pengumpulan data sebagai berikut:

   1. Wawancara yaitu sumber data yang digunakan adalah data primer yaitu data yang didapatkan dari lapangan atau pengumpulan data dengan melakukan wawancara semi terstruktur kepada Bank BNI Syariah dan Kapolres Lhokseumawe, untuk mendukung dan memperkuat hasil dari penelitian ini.
   2. Dokumentasi yaitu sumber data yang dikumpulkan dan dianalisis dalam penelitian ini. Dokumentasi dapat berupa kasus-kasus *cyber crime* yang menyerang nasabah, dokumentasi inilah yang akan memperjelas data-data yang didapatkan dari hasil wawancara.

b. Penelitian kepustakaan (*library research*) merupakan data sekunder yang digunakan untuk mendukung data primer,

dan dalam hal ini penulis mengadakan penelitian terhadap literatur yang ada kaitannya dengan penulisan skripsi ini, literatur ini berupa buku, majalah, surat kabar, internet, dan lain-lain yang berkaitan dengan tema skripsi ini.

3.4 Metode Analisis Data

Analisis data adalah upaya mencari dan menata dan secara sistematis, catatan hasil wawancara, dan observasi, dan lainnya untuk meningkatkan pemahaman tentang permasalahan yang diteliti. Dalam hal ini penulis menggunakan metode analisis data secara kualitatif. Analisis kualitatif dalam suatu penelitian digunakan apabila data penelitian yang diangkat dari lapangan juga memiliki sifat-sifat kualitatif. Hal ini dapat dilihat dari bagaimana morfologi dan strukur variabel penelitian serta tujuan penelitian yang semestinya dicapai (Bungin, 2013: 275).

3.4.1 Proses Pengolahan Data

Adapun setelah data terkumpul, maka dilakukan pengolahan dengan cara data tersebut dikumpulkan dan diamati terutama dari aspek kelengkapan, validasi serta relevansinya dengan tema pembahasan. Selanjutnya, diklasifikasi dan sistematisasi serta diformulasi sesuai dengan pokok permasalahan yang diteliti. Analisa yang dilakukan secara kualitatif berdasarkan data-data yang didapatkan dari wawancara dengan pihak Bank BNI Syariah dan Kapolres

Lhokseumawe. Adapun langkah-langkah dalam mengolah dan menganalisis data kualitatif:

1. Memvalidasi Data

Peneliti saat akan melakukan analisis data, terlebih dahulu memastikan apakah data yang ditemukan serta interpretasinya telah akurat atau belum. Validasi temuan dalam penelitian kualitatif menurut *Guba* (1981, *dalam Mills*, 2003), meliputi beberapa kriteria, yakni: *Credibility*, *Tranferability*, *Dependability*, dan *Confirmability* (Indrawan dan Yaniawati, 2014:153).

a. *Credibility* (kredibilitas) digunakan untuk mengatasi kompleksitas data yang tidak mudah untuk dijelaskan oleh sumber data. Peneliti harus berpartisipasi aktif dalam aktivitas kegiatan yang diamati, dan senantiasa berada ditempat penelitian sepanjang waktu penelitian (*prolonged participation at study site*), guna menghindari adanya bias dan persepsi yang salah. Dengan demikian, semua masalah dapat diatasi langsung di lapangan.

b. *Transferability* (keteralihan) merupakan konsep validitas yang menyatakan bahwa generalisasi suatu data penelitian dapat berlaku atau diterapkan pada konteks lain yang berkarakteristik sama (*representatif*). Hal ini juga dilakukan untuk membuktikan bahwa setiap data sesuai konteks,

artinya peneliti membuat deskripsi data secara detail dan mengembangkannya sesuai kondisi nyata yang dihadapi.

c. *Dependability* (ketergantungan) untuk menunjukkan stabilitas data, peneliti memeriksa dengan beberapa metode yang digunakan sehingga terjadi perbedaan antara data yang satu dengan yang lain. *Confirmability* (kepastian) untuk menunjukkan netralitas dan objektivitas data, peneliti dapat menggunakan jurnal untuk melakukan refleksi terhadap data yang dikumpulkan.

2. Mengorganisasi data dan Informasi

Langkah mengorganisasi data dan informasi mencakup tiga tahapan pekerjaan yakni transkripsi, reduksi data, dan koding data (Indrawan dan Yaniawati, 2014:154).

a. Trankripsi, adalah membuat uraian dalam bentuk tulisan yang rinci dan lengkap mengenai apa yang dilihat dan didengar, baik secara langsung maupun dari hasil rekaman. Proses kerja transkripsi menangkap makna dari teks untuk menunjukkan bagaimana makna dominan dalam teks, dan makna yang tersembuyi dalam teks. Akhirnya peneliti menganalisis bagaimana teks berkaitan dengan kehidupan, pengalaman, kenyataan, dan hal-hal yang bermakna tentang subjek penelitian.

b. Reduksi Data, adalah merangkum, memilih hal-hal yang pokok, yang memfokuskan pada hal-hal yang penting, serta dicari tema dan polanya. Dengan demikian, data yang telah di reduksi akan memberikan gambaran yang lebih jelas, dan mempermudah peneliti untuk melakukan pengumpulan data selanjutnya, dan mencarinya apabila di perlukan. Reduksi data dapat dibantu dengan peralatan, seperti komputer, *notebook* dan lain sebagainnya.

c. Koding Data, adalah kegiatan peneliti untuk mengelompokkan data dan memberi kode berdasarkan kesamaan data. Proses koding harus berlandaskan pada kerangaka teori yang dipilih. Teknik koding menurut Straus dan Corbin (2003), terdiri atas *open coding, axial coding, selective coding*.

   1) *Open Coding*, merupakan langkah pertama pemberian kode, dimana suatu gejala diidentifikasi berdasarkan kategorinya untuk kemudian diberikan atribut dan dimensi atau kategori tengah. Dalam artian sederhana open coding ini adalah proses merinci, menguji, membandingkan, konseptualisasi, dan melakukan ketegori data.

2) *Axial Coding* menghubungkan kategori gejala yang berhasil diidetifikasi satu sama lain. Kategori-kategori itu ada diposisikan sebagai, (a) penyebab, yaitu kejadian apapun yang menyebabkan terjadinya suatu gejala, (b) gejala itu sendiri, yaitu peristiwa sentral yang akan menggerakkan terjadinya serangkaian aksi/tindakan atau juga interaksi, (c) konteks, yaitu suatu kompleks kondisi, lokasi dan/atau waktu tertentu, yang menjadi ajang berlangsungnya suatu aksi atau interaksi, (d) kondisi peinterpensi, yaitu kondisi-kondisi struktural yang memudahkan atau menyulitkan jalannya proses dalam suatu konteks tertentu, (e) aksi atau interaksi, yaitu strategi tindakan yang dilakukan untuk merespon atau mengatasi permasalahan yang ada, (f) konsekuensi, yaitu hasil yang diperoleh lewat penyelenggaraan aksi atau interaksi.

3) *Selective Coding* merupakan proses untuk menyeleksi kategori-kategori guna menemukan kategori inti atau sentral. Kategori itu secara sistematis dapat dipakai secara konsepsional untuk merangkai dan mengintegrasikan kategori-kategori lain dalam suatu jaringan “paparan”.

Paparan panjang-lebar yang merupakan narasi tentang realita sosial yang diamati dan mengandung makna dinamai story. Proses mengintegrasikan kategori-kategori *selective coding*, yang berakhir dengan story, jauh lebih abstrak dan memiliki makna mendalam dibanding proses *axial coding*.

3. Menyajikan Temuan

Pada pendekatan kualitatif penyajian temuan, merupakan upaya peneliti melakukan paparan temuan dalam bentuk kategorisasi dan pengelompokan. Melalui penyajian data tersebut, maka data terorganisasikan dan tersusun dalam pola hubungan, sehingga tergambarkan kaitan antara satu kejadian dengan kejadian yang lain, atau satu perilaku dengan perilaku lain, baik dimasa lalu maupun kemungkinan dimasa depan, dalam bentuk narasi saat penyajian temuan perlu diperhatikan beberapa konsep yakni deskripsi, tematik, diskusi narasi (Indrawan dan Yaniawati, 2014:156).

4. Validasi Temuan

Validasi temuan menurut Creswell (2012) merupakan penentuan tingkat akurasi dan kredibilitas temuan melalui beberapa strategi antara lain member *checking*, *triangualation*, dan *auditing* (Indrawan dan Yaniawati, 2014:159).

a. *Member Checking*, dilakukan dengan cara kembali ke *research setting* untuk memverifikasi kredibilitas informasi. Dengan asumsinya adalah, (a) setiap temuan harus didiskusikan dan dicek validitasnya dengan orang dalam organisasi yang mengetahui fenomena yang diteliti, (b) apakah temuan yang dihasilkan atau diinterpretasikan sama baiknya oleh peneliti yang lain.

b. *Triangulation*, artinya menggunakan berbagai pendekatan dalam melakukan penelitian. Dalam penelitian kualitatif peneliti dapat menggunakan berbagai sumber data, teori, metode, agar data dan informasi dapat diinterpretasikan secara konsisten. Oleh karena itu, untuk memahami dan mencari jawaban atas pertanyaan penelitian, peneliti dapat menggunakan lebih dari satu teori, lebih dari satu metode (interview, observasi dan analisis dokumen).

c. *Auditing*, dapat dilakukan dengan cara peneliti mengkonsultasikan hasil temuan penelitian dengan pihak eksternal yang dipilih adalah orang yang memahami fenomena yang diamati dan independen serta memiliki konpetensi.

5. Menafsirkan dan Teorisasi Temuan

Menafsirkan atau teorisasi pada dasarnya upaya subjektif peneliti untuk mengomunikasikan hasil penelitian dengan melibatkan "rasa data", atau memberi "pelajaran". Penelitian kualitatif adalah penelitian interpretatif, dan peneliti perlu untuk memahami temuan" implikasi". Bagian ini berisi antara lain, (a) temuan utama yang merupakan jawaban atas pertanyaan penelitian, (b) refleksi subjektif peneliti tentang makna data, (c) pendapat pribadi peneliti yang merupakan perbandingan dengan literatur yang ada, (d) keterbatasan penelitian, (e) saran untuk penelitian masa depan (Indrawan dan Yaniawati, 2014:160).

3.4.2 Teknik Analisa Data

Analisis data adalah proses mengorganisasikan dan mengurutkan data kedalam pola, kategori, dan saruan uraian dasar sehingga dapat ditemukan tema dan dapat dirumuskan hipotesis kerja seperti yang disarankan oleh data. Aktivitas dalam analisis data diskriptif melalui tiga cara yaitu:

1. Reduksi Data (*data reduction*)

Mereduksi data adalah merangkum, memilih hal-hal yang pokok, memfokuskan pada hal-hal yang penting, dicari tema dan polanya. Dengan demikian data yang telah direduksi akan memberikan gambaran yang lebih jelas, dan mempermudah peneliti untuk melakukan pengumpulan data selanjutnya dan mencarinya bila di perlukan.

2. Penyajian Data (*data display*)

Setelah data direduksi maka langkah selanjutnya adalah mendisplaikan data yang dapat dilakukan dalam bentuk tabel, grafik, pictogram dan sejenisnya. Melalui penyajian data tersebut maka data terorganisasikan, tersusun dalam pola hubungan, sehingga akan semakin mudah dipahami dalam rangka memperoleh kesimpulan sebagai temuan penelitian.

3. Penarikan Kesimpulan atau Verifikasi (*conclusion drawing/verivication*)

Langkah ketiga dalam analisis data kualitatif adalah penarikan kesimpulan dan verifikasi. Kesimpulan awal yang dikemukakan masih bersifat sementara, dan akan berubah bila tidak ditemukan bukti-bukti yang kuat yang mendukung pada tahap pengumpulan data berikutnya. Tetapi apabila kesimpulan yang dikemukakan pada tahap awal, didukung oleh bukti-bukti yang valid dan konsisten saat peneliti kembali ke lapangan mengumpulkan data, maka kesimpulan yang dikemukakan merupakan kesimpulan yang akurat (Moleong, 2000)

3.5 Lokasi Penelitian

Lokasi penelitian adalah tempat dimana penelitian dilakukan. Penetapan lokasi penelitian merupakan tahap yang sangat penting dalam penelitian kualitatif, karena dengan diterapkannya lokasi penelitian berarti objek dan tujuan sudah ditetapkan sehingga mempermudah penulis dalam melakukan penelitian. Pemilihan

lokasi penelitian oleh peneliti dikarenakan tempat yang di teliti merupakan tempat yang tepat untuk dikaitkan dengan judul penelitian.

Lokasi penelitian ini bertempat di salah satu Cabang Bank BNI Syariah Lhokseumawe. Alasan penulis memilih Cabang Bank BNI Syariah Lhokseumawe yaitu karena bank tersebut sudah pernah terjadinya kasus kejahatan *cyber crime* yang menyerang nasabah. Adapun alasan lainnya yaitu pengelolaan dan pelayanan yang di berikan oleh Bank BNI Syariah dengan sangat baik, sehingga menjadi daya tarik penulis untuk menjadikan Bank BNI Syariah sebagai tempat penelitian yang tepat.

BAB IV
HASIL PENELITIAN DAN PEMBAHASAN

4.1 Gambaran Umum BNI Syariah

4.1.1 Sejarah Berdirinya BNI dan BNI Syariah

Sejak awal didirikan pada tanggal 5 Juli 1946, sebagai Bank Pertama yang secara resmi dimiliki Negara RI, BNI merupakan pelopor terciptanya berbagai produk dan layanan jasa perbankan. BNI terus memperluas perannya, tidak hanya terbatas sebagai bank pembangunan, tetapi juga ikut melayani kebutuhan transaksi perbankan masyarakat umum dengan berbagi segmentasinya, mulai dari Bank Terapung, Bank Sarinah (bank khusus perempuan) sampai dengan Bank Bocah khusus anak-anak. Seiring dengan pertambahan usianya yang memasuki 67 tahun, BNI tetap kokoh berdiri dan siap bersaing di industri perbankan yang semakin kompetitif. Dengan semangat "Tak Henti Berkarya" BNI akan terus berinovasi dan berkreasi, tidak hanya terbatas pada penciptaan produk dan layanan perbankan, bahkan lebih dari itu BNI juga bertekad untuk menciptakan "*value*" pada setiap karyanya (Bni, 2014).

Berdiri sejak 1946, BNI yang dahulu dikenal sebagai Bank Negara Indonesia, merupakan Bank pertama yang didirikan dan dimiliki oleh Pemerintah Indonesia (Bni 2014). Sejalan dengan keputusan penggunaan tahun pendirian sebagai bagian dari

identitas perusahaan, nama Bank Negara Indonesia 1946 resmi digunakan mulai akhir tahun 1968. Perubahan ini menjadikan Bank Negara Indonesia lebih dikenal sebagai "BNI 46" dan ditetapkan bersamaan dengan perubahan identitas perusahaan tahun 1988. Dari tahun ke tahun BNI selalu menunjukkan kekuatannya dalam industri perbankan dan kepercayaan masyarakat pun terbangun dalam memilih Bank Negara Indonesia sebagai pilihan tempat penyimpanan segala alat kekayaan yang terpercaya. Permintaan akan perbankan yang sesuai dengan prinsip syariah pun mulai bermunculan yang pada akhirnya BNI membuka layanan perbankan yang sesuai dengan prinsip syariah dengan konsep *dual system banking*, yakni menyediakan layanan perbankan umum dan syariah sekaligus. Hal ini sesuai dengan UU No. 10 Tahun 1998 yang memungkinkan bank-bank umum untuk membuka layanan syariah, diawali dengan pembentukan Tim Bank Syariah di Tahun 1999, Bank Indonesia kemudian mengeluarkan izin prinsip dan usaha untuk beroperasinya unit usaha syariah BNI. Setelah itu BNI Syariah menerapkan strategi pengembangan jaringan cabang, syariah sebagai berikut:

a. Tepatnya pada tanggal 29 April 2000 BNI Syariah membuka 5 kantor cabang syariah sekaligus di kota-kota potensial, yakni: Yogyakarta, Malang, Pekalongan, Jepara dan Banjarmasin.

b. Tahun 2001 BNI Syariah kembali membuka 5 kantor cabang syariah yang difokuskan ke kota-kota besar di Indonesia, yaitu : Jakarta (2 cabang), Bandung, Makassar, dan Padang.
c. Seiring dengan perkembangan bisnis dan banyaknya permintaan masyarakat untuk layanan perbankan syariah, tahun 2002 lalu BNI Syariah membuka dua kantor cabang syariah baru di Medan dan Palembang.
d. Di awal tahun 2003, dengan pertimbangan load bisnis yang semakin meningkat sehingga untuk meningkatkan pelayanan kepada masyarakat, BNI Syariah melakukan relokasi kantor cabang syariah dari Jepara ke Semarang. Sedangkan untuk melayani masyarakat kota Jepara, BNI Syariah membuka Kantor Cabang Cabang Pembantu Syariah Jepara.
e. Pada bulan Agustus dan September 2004, BNI Syariah membuka layanan BNI Syariah Prima di Jakarta dan Surabaya. Layanan ini diperuntukkan untuk individu yang membutuhkan layanan perbankan yang lebih personal dalam suasana yang nyaman. Dari awal beroperasi hingga kini, BNI Syariah menunjukkan pertumbuhan yang signifikan. Disamping itu komitmen Pemerintah terhadap pengembangan perbankan syariah semakin kuat dan kesadaran terhadap keunggulan produk perbankan syariah juga semakin meningkat.

4.1.2 Visi dan Misi BNI Syariah

1. Visi

Menjadi bank syariah pilihan masyarakat yang unggul dalam layanan dan kinerja.

2. Misi

1. Memberikan kontribusi positif kepada masyarakat dan peduli pada kelestarian lingkungan.
2. Memberikan solusi bagi masyarakat untuk kebutuhan jasa perbankan syariah.
3. Memberikan nilai investasi yang optimal bagi investor.
4. Menciptakan wahana terbaik sebagai tempat kebanggaan untuk berkarya dan berprestasi sebagai pegawai sebagai perwujudan ibadah.
5. Menjadi acuan tata kelola perusahaan yang amanah.

4.1.3 Deskripsi Tugas

1. Cabang/Direksi

Terdiri dari seorang pemimpin cabang, direksi memimpin serta mengawasi kegiatan bank sehari-hari sesuai dengan kebijaksanaan umum yang telah disetujui dalam anggaran dasar. Tugas dan tanggung jawab

1. Merumuskan dan mengusulkan kebijaksanaan umum bank untuk masa yang akan datang kepada dewan komisaris agar tercapai tujuan kontinuitas operasional perusahaan.

2. Menyusun dan mengusulkan rencana anggaran perusahaan dan rencana kerja untuk tahun buku yang baru kepada dewan komisaris.
3. Mengajukan rencana dan perhitungan laba rugi tahunan serta laporan-laporan berkala lainnya kepada dewan komisaris untuk mendapatkan penilaian.
4. Menyetujui pemindah tangan saham–saham kepada pemilik baru yang ditujukan atau dipilih oleh pemegang saham lama, setelah mengikuti prosedur yang ditetapkan dalam anggaran dasar mengenai pemindah tanganan saham-saham.
5. Mengundang pemegang saham untuk menghadiri RUPS.
6. Mengajukan kepada dewan komisaris, jenis pelayanan baru yang dapat diberikan bank kepada masyarakat untuk disetujui.
7. Memberi persetujuan atas penggunaan formulir-formulir dan dokumen-dokumen lainnya dalam transaksi-transaksi bank.
8. Menyetujui pembiayaan yang jumlahnya tidak melampaui batas wewenang direksi.
9. Mengangkat pejabat-pejabat bank yang akan diberi tanggung jawab untuk mengawasi kegiatan bank.
10. Menyetujui besarnya gaji dan tunjangan lainnya yang harus dibayarkan kepada pejabat dan pegawai bank.

11. Mengamankan harta kekayaan bank agar terlindungi dari bahaya kebakaran, pencurian, perampokan dan kerusakan.
12. Melaksanakan tugas-tugas lain yang diberikan oleh dewan komisaris.
13. Menyusun dan tanggung jawab atas penyusunan rencana kerja yang dituangkan dalam rencana kerja bank yang akan disampaikan kepada Bank Indonesia.
14. Melaksanakan langkah-langkah perbaikan atas ketidaksesuaian dalam penyaluran dana yang ditemui oleh SKAI (Satuan Kerja Audit Internal).
15. Melaksanakan ketaatan bank terhadap ketentuan perundang-undangan dan peraturan yang berlaku. Melaporkan secara berkala dan tertulis kepada komisaris disertai langkah-langkah perbaikan yang telah, sedang dan sekurang-kurangnya mengenai:
    a. Perkembangan dan kualitas portofolio penyaluran dana secara keseluruhan.
    b. Perkembangan dan kualitas penyaluran dana yang diberikan kepada pihak yang terkait maupun yang tidak terkait.
    c. Temuan-temuan penting dalam penarikan dana yang dilaporkan SKAI.

d. Pelaksanaan operasional kerja sebagaimana telah tertuang dalam rencana kerja bank yang disampaikan kepada Bank Indonesia.

2. Account Officer/Relationship Officer

Tugas dan tanggung jawab

1. Melakukan survei dan prospek terhadap nasabah yang mengajukan pembiayaan.
2. Melakukan analisa setelah melakukan survei/prospek terhadap data-data yang dipakai dalam pengajuan pembiayaan.
3. Melakukan pantauan dan pembinaan terhadap aktifitas nasabah.
4. Memberikan surat peringatan kepada nasabah yang lalai atau wanprestasi terhadap akad.

3. Manager Operasional

Tugas dan tanggung jawab

1. Membantu terlaksananya tugas direksi dan bagian-bagian lainnya dalam pengadaan sarana operasional dan fasilitas-fasilitas lainnya.
2. Memantau perkembangan asset dan likuiditas perusahaan.
3. Melakukan checker terhadap transaksi yang sesuai dengan ketentuan perusahaan.

4. Mengerjakan dan bertanggung jawab terhadap pekerjaan teller, accounting, admin PYD/legal dan umum jika yang bersangkutan berhalangan hadir.
5. Memback-up semua bagian operasional jika ada bagian tugas tertentu di dalam operasional yang diadakan.
6. Melakukan koordinasi dengan bagian marketing untuk kelancaran operasional sehari-hari. Wewenang:
    1. Mengarahkan personil untuk melancarkan operasional.
    2. Mengawasi sistem dan prosedur operasional yang dijalankan.

4. Hukum/Administrasi Umum Tugas dan tanggung jawab
    1. Mengkoordinir dan mengawasi semua aktifitas yang berhubungan dengan pembiayaan.
    2. Mengikuti perkembangan proses permohonan pembiayaan setiap nasabah dalam hal pemeriksaan kelengkapan dokumen pembiayaan.
    3. Mengurus kelengkapan dokumen yang berhubungan dengan pembiayaan yang akan atau telah diberikan kepada nasabah seperti surat-surat perjanjian pembiayaan, surat-surat jaminan dan sebagainya sampai dengan pembiayaan cair.
    4. Mengawasi dan mengatur pengarsipan terhadap semua dokumen yang berhubungan dengan pembiayaan menurut sistem dan data yang telah ditentukan.

5. Mengatur peminjaman arsip dokumen kepada pegawai berwenang dan menghindari kerusakan atau kehilangan atas dokumen dokumen tersebut.
6. Menyiapkan dan membuat surat-surat pengikatan atau pembiayaan yang telah disetujui.
7. Menyimpan akte pendirian bank dan perubahannya.
8. Melakukan peninjauan kelengkapan baik bersama manager marketing/coordinator wilayah mengenai data-data permohonan pembiayaan dengan kondisi sebenarnya.
9. Menilai secara jaminan pembiayaan yang diajukan oleh nasabah.
10. Mengatur pelaksanaan eksekusi jaminan.
11. Mengajukan dan menjawab perkara bila sampai ke pengadilan.
12. Membantu direksi dalam perbuatan surat-surat yang berhubungan dengan administrasi umum.

Setiap bagian tersebut di atas, satu dengan yang lainnya selalu mengadakan konsolidasi terhadap aktifitas perbankan.

4.1.4 Tujuan Bank BNI Syariah

Sesuai dengan Anggaran Dasar Perusahaan No. 160 tanggal 22 Maret 2010, maksud dan tujuan BNI Syariah adalah menyelenggarakan usaha perbankan berdasarkan prinsip syariah sesuai dengan ketentuan dalam peraturan perundang-

undangan yang berlaku. Sedangkan kegiatan usaha BNI Syariah antara lain mencakup hal-hal sebagai berikut:

1. Menghimpun dana dalam bentuk simpanan berupa giro, tabungan, atau bentuk lainnya yang dipersamakan dengan itu berdasarkan akad *wadi'ah* atau akad lain yang tidak bertentangan dengan prinsip syariah;
2. Menghimpun dana dalam bentuk investasi berupa deposito, tabungan, atau bentuk lainnya yang dipersamakan dengan itu berdasarkan akad mudarabah atau akad lain yang tidak bertentangan dengan prinsip syariah;
3. Menyalurkan pembiayaan bagi hasil berdasarkan akad mudarabah, akad musyarakah, atau akad lain yang tidak bertentangan dengan prinsip syariah;
4. Menyalurkan pembiayaan berdasarkan akad murabahah, akad *salam*, akad *istishna'*, atau akad lain yang tidak bertentangan dengan prinsip syariah;
5. Menyalurkan pembiayaan berdasarkan akad *qardh* atau akad lain yang tidak bertentangan dengan prinsip syariah;
6. Menyalurkan pembiayaan penyewaan barang bergerak atau tidak bergerak kepada nasabah berdasarkan akad ijarah dan/ atau sewa beli dalam bentuk *ijarah muntahiya bittamlik* atau akad lain yang tidak bertentangan dengan prinsip syariah;

7. Melakukan pengambilalihan utang berdasarkan akad *hawalah* atau akad lain yang tidak bertentangan dengan prinsip syariah;
8. Melakukan usaha kartu debit dan/atau kartu pembiayaan berdasarkan prinsip syariah;
9. Membeli, menjual, atau menjamin atas risiko sendiri surat berharga pihak ketiga yang diterbitkan atas dasar transaksi nyata berdasarkan prinsip syariah antara lain, seperti akad ijarah, musyarakah, mudarabah, murabahah, *kafalah*, atau *hawalah*;
10. Membeli surat berharga berdasarkan prinsip syariah yang diterbitkan oleh pemerintah dan/atau Bank Indonesia;
11. Menerima pembayaran dari tagihan atas surat berharga, dan melakukan perhitungan dengan pihak ketiga atau antar pihak ketiga berdasarkan prinsip syariah;
12. Melakukan penitipan untuk kepentingan pihak lain berdasarkan suatu akad yang berdasarkan prinsip syariah;
13. Menyediakan tempat untuk menyimpan barang dan surat berharga berdasarkan prinsip syariah;
14. Memindahkan uang, baik untuk kepentingan sendiri maupun kepentingan nasabah berdasarkan prinsip syariah;

15. Melakukan fungsi sebagai wali amanat berdasarkan akad *wakalah*;
16. Memberikan fasilitas *letter of credit* atau bank garansi berdasarkan prinsip syariah;
17. Melakukan kegiatan lain yang lazim dilakukan di bidang perbankan dan bidang sosial sepanjang tidak bertentangan dengan prinsip syariah dan sesuai dengan ketentuan peraturan perundang-undangan.

Selain melakukan kegiatan usaha tersebut, BNI Syariah dapat pula:

1. Melakukan kegiatan dalam valuta asing berdasarkan prinsip syariah;
2. Melakukan kegiatan penyertaan modal pada Bank Umum Syariah atau lembaga keuangan yang melakukan kegiatan usaha berdasarkan prinsip syariah;
3. Melakukan kegiatan penyertaan modal sementara untuk mengatasi akibat kegagalan pembiayaan dengan syarat harus menarik kembali penyertaannya sesuai dengan ketentuan yang ditetapkan Bank Indonesia;
4. Bertindak sebagai pendiri dan pengurus dana pensiun berdasarkan prinsip syariah;
5. Melakukan kegiatan dalam pasar modal sepanjang tidak bertentangan dengan prinsip syariah dan ketentuan peraturan perundang-undangan di bidang pasar modal;

6. Menyelenggarakan kegiatan atau produk bank yang berdasarkan prinsip syariah dengan menggunakan sarana elektronik;
7. Menerbitkan, menawarkan dan memperdagangkan surat berharga jangka pendek berdasarkan prinsip syariah, baik secara langsung maupun tidak langsung melalui pasar uang;
8. Menerbitkan, menawarkan dan memperdagangkan surat berharga jangka panjang berdasarkan prinsip syariah, baik secara langsung maupun tidak langsung melalui pasar modal; dan
9. Menyediakan produk atau melakukan kegiatan jasa keuangan, *commercial banking*, dan *investment banking* lainnya berdasarkan prinsip syariah (bnisyariah, 2014).

4.2 Hasil Penelitian

4.2.1 Faktor-Faktor Yang Menyebabkan Kejahatan *Cyber Crime* di Bank BNI Syariah

Berdasarkan data di Mabes Polri, terdapat 2 jenis kategori kejahatan, yaitu kejahatan yang menjadikan sistem dan jaringan komputer sebagai sarana kejahatan dan kejahatan yang menggunakan komputer sebagai sarana, kedua kategori kejahatan tersebut dikenal dengan istilah kejahatan yang berhubungan dengan computer (*computer-related crime*). Bentuk kejahatan yang berhubungan dengan komputer yang paling banyak terjadi di

Indonesia adalah pemalsuan kartu kredit *(carding)* dan secara berurutan, dari jumlah kasus yang terbesar ke yang terkecil adalah kasus *terorism, cracking, Banking, Fraud, DoS/DdoS attack, Pornography, Illegal access,* pelanggaran hak cipta, penjiplakan situs (*typosquatting*), *Hacking,* penyebaran virus (*worm*), pencucian uang (*money loundering*), dan penggunaan jaringan internet milik pihak lain secara tidak sah (*phreaking*). Jumlah kejahatan komputer terbesar terjadi pada tahun 2002, yaitu 126 kasus, sedangkan jumlah terkecil terjadi pada tahun 2001, yaitu hanya 11 kasus (*cyber crime* mabes polri, 2006).

Berdasarkan hasil wawancara dengan Dicky Patrianegara selaku komisaris polisi yang bertugas sebagai penyidik *cyber crime* penyebab pelaku kejahatan yang berhubungan dengan komputer sangat bervariasi, tergantung pada bentuk kejahatan yang dilakukan dan karakteristik pribadi pelaku kejahatan. Untuk kejahatan *cyber crime* tersebut terdiri dari faktor-faktor sebagai berikut:

a. Saat ini ada perubahan motivasi melakukan kejahatan. Jika dahulu para pelaku *cracking, Denial service* (*DoS*) *Attack* atau *Distributed Denial Service* (*DDoS*) *Attack* atau kejahatan lain terhadap sistem atau jaringan komputer melakukan kejahatan karena merasa tertantang dengan teknologi, mencoba keandalan pengamanan sistem komputer pihak lain, dan bersenang-senang, saat ini banyak pihak termotivasi untuk memperoleh imbalan berupa uang (motivasi ekonomi). Saat ini seorang *Cracker* dapat melakukan *Cracking* karena

diberi upah oleh orang pihak lain Motivasi pihak yang menyuruh *Cracker* (pemilik uang) antara lain balas dendam (karena situs miliknya pernah diserang), persaingan usaha, untuk mengetahui rahasia dagang pihak lain.

b. Dalam kasus *typosquating* (kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain) diharapkan agar para pengguna *e-bangking* dalam bertransaksi lebih berhati-hati dalam memasukkan PIN dan identitas pengguna (*user identity*), meskipun seringkali terjadi penipuan.
c. Dalam kasus-kasus yang dapat mendatangkan keuntungan berupa uang, misalnya *carding*, penipuan melalui bank (transfer uang secara fiktif, transfer uang tanpa hak), tindak pidana korupsi, penyalahgunaan nama domein, pelanggaran hak cipta, dan *phishing*, sebagian besar pelaku didorong oleh motif untuk mendapatkan uang secara melawan hukum.
d. Motif politik dapat juga mendorong tindakan *cracking* dan *defacing*, dan *DoS Attack*, misalnya pada saat antara Indonesia dengan Malaysia sedang membicarakan status Kepulauan Ambalat tahun 2005. Motif kekecewaan sekelompok orang atau sekelompok *craker* dapat memacu kejahatan yang berhubungan dengan komputer.

Adapun terkait dengan kejahatan *cyber crime* di Bank BNI Syariah berdasarkan hasil wawancara, yaitu penulis melakukan

wawancara dengan beberapa pihak. Berikut adalah hasil wawancara penulis:

Wawancara dengan ibu Melia Indri, yang merupakan salah satu pegawai negeri sipil yang bertugas di Kasat Reskrim Polres Lhokseumawe. Dalam pernyataannya ibu Melia Indri mengatakan: "Kejahatan dunia maya atau sering dikenal dengan sebutan kejahatan cyber crime ini dapat terjadi melalui beberapa faktor, seperti faktor ekonomi dimana rendahnya pendidikan seseorang sehingga mendorong dirinya untuk mencari jalan pintas agar mendapatkan penghasilan demi memenuhi kebutuhannya. Dan juga dari faktor lingkungan, dimana tingkat pergaulan menentukan pembentukan mental dan karakter seseorang. Seseorang yang bahkan tidak pernah melakukan pelanggaran hukum, maka cenderung akibat bergaul dengan seseorang yang sering melakukan pelanggaran hukum, maka orang tersebut akan tergolong menjadi bagaian dari seseorang yang melakukan pelanggaran hukum itu juga"

4.2.2 Kebijakan Bank BNI Syariah dalam menangani kejahatan *cyeber crime*

Dalam kamus besar bahasa Indonesia (KBBI) Kebijakan adalah rangkaian konsep dan asas yang menjadi pedoman dan dasar rencana dalam pelaksanaan suatu pekerjaan, kepemimpinan, dan cara bertindak. Istilah ini dapat diterapkan pada pemerintahan, organisasi dan kelompok sektor swasta, serta individu. Kebijakan

berbeda dengan peraturan dan hukum. Jika hukum dapat memaksakan atau melarang suatu perilaku (misalnya suatu hukum yang mengharuskan pembayaran pajak penghasilan), kebijakan hanya menjadi pedoman tindakan yang paling mungkin memperoleh hasil yang diinginkan.

Adapun penerapan dalam penanganan komplain Nasabah akibat tindak kejahatan eksternal (investigation unit) kinerja investigation unit tahun 2017 dalam penanganan pengaduan nasabah terkait tindak kejahatan eksternal cukup tinggi, hal tersebut dipengaruhi oleh era digital *banking* yang memudahkan masyarakat menggunakan fasilitas *e-channel* untuk semua transaksi perbankan kapanpun dan dimanapun, hal tersebut berpotensi dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan kejahatan secara ekternal diantaranya kasus *trapping, skimming, pharming, phising* dan ancaman *cyber crime*.

Penanganan kasus penipuan di unit *e-banking* dibagi menjadi 2 sumber yaitu penanganan pengaduan internal dan eksternal.

1. Penanganan pengaduan Nasabah secara internal pengaduan Nasabah BNI Syariah melalui seluruh cabang regular dan cabang mikro terintegrasi pada *Handling Complain System* (HCS) yang di kelola oleh kantor pusat. SLA penyelesaian pengaduan Nasabah mengacu pada ketentuan peraturan otorisasi jasa keuangan No: 1/ POJK.07/2013 Pasal 35. Penyelesaian pengaduan dilakukan oleh kantor pusat yang

kemudian disampaikan ke cabang melalui HCS untuk kemudian disampaikan kepada Nasabah.

2. Penanganan pengaduan Nasabah secara eksternal sumber pengaduan unit *e-banking* secara eksternal diantaranya berasal dari : i) BNI *Call Center* ii) pengaduan dari bank lain melalui media email atau surat Berdasarkan data pengaduan yang di terima unit *e-banking*, penyelesaian pengaduan secara eksternal dilakukan dengan menganalisis terlebih dahulu transaksi yang dilaporkan antar bank, selanjutnya dilakukan informasi antar bank dengan menggunakan surat resmi / surat bilateral dan *indemnity letter* apabila dana masih dapat di kembalikan dari rekening terlapor. Hal ini dilakukan untuk tetap menjaga hubungan baik dengan bank lain serta menjaga nama baik BNI Syariah (*Corporate Image*).

Tabel 4.1

Penanganan pengaduan Nasabah internal dan eksternal tahun 2017

No	Jenis kejahatan	Pengaduan masuk	Pengaduan diselesaikan	Pending
1	*Trapping*	11	11	
2	*Skimming*	25	24	1
3	*Phising*	8	8	
4	*Pharming*	12	12	
5	Kasus penipuan (antar bank)	209	209	
	Jumlah	265	264	1

Sumber: Data diolah (2020)

Berdasarkan tabel di atas dapat ditarik kesimpulan sebagai berikut :

1. Total pengaduan Nasabah melalui internal dan eksternal unit *e-banking* pada tahun 2017 sebanyak 265 pengaduan. Selama tahun 2017 berhasil diselesaikan 264 pengaduan, terdapat sisa 1 pengaduan yang belum diselesaikan dikarenakan belum terpenuhi syarat-syarat pengaduan oleh Nasabah.
2. Jenis kejahatan eksternal didominasi dengan kasus skimming card, banyak terjadi pada tahun 2017 di beberapa daerah diantaranya Mataram, Pekanbaru dan Jakarta Timur. Namun sudah ada pelaku yang tertangkap yaitu kasus *skimming card* di daerah Jakarta Timur, hal tersebut sebagai tindak lanjut nyata upaya penanganan pengaduan Nasabah dari unit *e-banking*.
3. Kasus penipuan antar bank merupakan pengaduan Nasabah eskternal dimana rekening Nasabah digunakan sebagai rekening penampungan untuk penipuan. Pada tahun 2017 cukup banyak kasus penipuan (antar bank) kasus pengaduan di dominasi oleh kasus jual beli secara online.

User-Id BNI *e-banking* dapat mengakses semua rekening yang terdapat dalam 1 (satu) CIF nasabah namun yang digunakan sebagai *account base* (*rekening debet*) untuk transaksi finansial adalah rekening yang terafiliasi dengan BNI Card yang digunakan saat registrasi layanan BNI *e-banking* di BNI ATM. Selain *account base* yang terafiliasi dengan BNI Card, nasabah dapat menggunakan rekeningnya yang lain

dalam 1 (satu) CIF sebagai rekening debet transaksi finansial BNI *e-banking* dengan cara melakukan pendaftaran ke Kantor Cabang terdekat. Kerahasiaan User-Id dan Password BNI *e-banking* adalah sepenuhnya menjadi tanggung jawab Pengguna BNI *e-banking* dan hanya boleh digunakan oleh Pengguna BNI *e-banking* yang bersangkutan. Pengguna BNI *e-banking* wajib mengamankan *User-Id* dan *Password* BNI *e-banking* dengan cara :

1. Berhati-hati dalam menggunakan *User-Id* dan *Password* BNI *e-banking* agar tidak diketahui oleh orang lain.
2. Tidak memberitahukan *User-Id* dan *Password* BNI *e-banking* kepada orang lain termasuk kepada anggota keluarga atau sahabat untuk tujuan apapun.
3. Tidak menuliskan *User-Id* dan *Password* BNI *e-banking* atau menyimpannya dalam bentuk tertulis atau sarana penyimpanan lainnya sehingga memungkinkan untuk diketahui oleh orang lain.
4. Tidak menggunakan *User-Id* dan *Password* BNI *e-banking* yang diberikan oleh orang lain atau yang mudah diterka seperti tanggal lahir atau kombinasinya,nomor telepon dan lain-lain.
5. Penyalahgunaan *User-Id* dan *Password* BNI *e-banking* merupakan tanggung jawab nasabah Pengguna BNI *e-banking* yang bersangkutan dan membebaskan BNI dari segala tuntutan yang timbul baik dari Pengguna BNI *e-*

banking maupun pihak lain sebagai akibat penyalahgunaan tersebut. Pada saat aktivasi, Pengguna BNI *e-banking* diberi kebebasan untuk membuat *User-Id* dan *Password*-nya sendiri dan dapat melakukan perubahan/ penggantian *Password* tersebut apabila ada kecurigaan diketahui oleh orang lain.

Adapun terkait dengan kejahatan *cyber crime* di Bank BNI Syariah berdasarkan hasil wawancara, yaitu penulis melakukan wawancara dengan beberapa pihak. Berikut adalah hasil wawancara penulis:

Wawancara dengan Bapak Hanafi, yang merupakan salah satu pegawai Bank BNI Syariah yang bertugas dibagian staf administrasi. Dalam pernyataannya bapak Hanafi mengatakan: "Dari pengaduan Nasabah atas kehilangan uang mereka dalam rekeningnya, kasus cyber crime yang pernah terjadi di Bank BNI Syariah ini adalah kasus Skimming dimana uang di rekening Bank mereka tiba-tiba berkurang. Sehingga upaya yang bisa diambil dalam penanganan kasus ini di harapkan kepada Nasabah agar tidak bertransaksi Internet Banking menggunakan computer di tempat umum, dan selalu memperhatikan notifikasi transaksi pada Internet Banking serta tidak mudah memberikan data pribadi berupa token/user id/password kepada pihak lain."

BAB V
PENUTUP

5.1 Kesimpulan

Dari hasil penulisan skripsi yang telah penulis kerjakan, maka penulis dapat menarik kesimpulan yaitu:

a. 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. Dan juga dari faktor lingkungan, akibat pergaulan seseorang sehingga memungkinkan seseorang tersebut bisa terjerumus kedalam tindak kejahatan *cyber crime* ini.
b. Kebijakan Bank BNI Syariah dalam menangani kasus *cyber crime* ini ialah dengan cara mendorong para Nasabahnya agar lebih berhati-hati dalam melakukan transaksi online, dan selalu menjaga keamanan *pasword/user id* agar tetap aman dan tidak tersebar kepada pihak lain.

5.2 Saran

Berdasarkan pembahasan dan kesimpulan yang penliti paparkan, peneiliti memberikan beberapa saran berkaitan dengan kejahatan *cyber crime:*

1. Pihak Perbankan

   Disarankan kepada pihak perbankan untuk dapat melakukan inovasi teknologi yang dapat memaksimalkan

tingkat keamanan terhadap kejahatan *cyber crime* yang pada akhirnya dapat menimbulkan rasa aman dari masyarakat.

2. Pihak Pemerintah

   Disarankan kepada pemerintah untuk dapat berkoordinasi dengan pihak media baik media offline maupun media online untuk dapat mempublikasikan keberadaan peraturan mengenai tindak pidana *cyber crime* mengingat masih ada orang yang bahkan belum cukup mengerti tentang peraturan mengenai tindak pidana tersebut.

3. Pihak Masyarakat

   Disarankan kepada masyarakat serta pembaca untuk dapat lebih berhati-hati dalam menggunakan kartu kredit pada saat melakukan pembelanjaan menggunakan kartu kredit baik offline maupun online mengingat pada saat ini era teknologi, modus operandi yang dipakai para *carder* dalam melakukan tindak pidana intersepsi atau penyadapan kartu kredit sangatlah beragam dan sulit terdeteksi.

DAFTAR PUSTAKA

Abidin ZD, (2015), *Kejahatan Dalam Teknologi Informasi dan Komunikasi*, Ilmiah Media Profesor, No 2, Vol 10.

Akurat, (2018), *Kejahatan Skimming Makin Menggila*, https://akurat.co/ekonomi/id-193225-read-kejahatan-skimming-makin-menggila-begini-solusi-menurut-polisi, 28 Agustus 2019.

Arief B.N, (2003), *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana, Bandung*.

Bni, (2014), *Sejarah*, https://www.bni.co.id/id-id/perusahaan/tentangbni/sejarah, 5 September 2019.

Bnisyariah, (2014), *Kegiatan Usaha dan Produk*, PT Bank BNI Syariah, 5 September 2019.

Bnisyariah, 2016, *Mekanisme Pengaduan Nasabah*, PT BNI Syariah, No 186

Bnisyariah, (2017), *Perubahan Manajemen BNI Syariah*, https://www.bnisyariah.co.id/id-id/beranda/berita/siaranpers/ArticleID/869/Perubahan-Manajemen-BNI-Syariah, 29 Agustus 2019

Bungin, B. 2013. *Penelitian Kualitatif. Komunikasi, Ekonomi, Kebijakan Publik, dan Ilmu sosial lainnya*. Jakarta: Kencana Predana Media Group.

Burhan, Bungin, 2001, *Metodologi Penelitian Sosial*,

Airlangga University Surabaya.

Creswell, J. W (2012), *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research, 4th edition, Pearson Education, Boston.*

Cyber Crime Mabes Polri, 2006, *Daftar Perkara Cyber Crime, Inpotek*, Unit V

Faridi K.M, 2018, *Kejahatan Cyber Dalam Bidang Perbankan, Cyber Security* dan *Forensik Digital*, No 2, Vol 1.

Gema A.J, 2013, *Cybercrime: Sebuah Fenomena di Dunia Maya*, www.interpol.go.id, 3 September 2019

Ghony M.D, Almanshur Fauzan, 2012, *Metode Penelitian Kualitatif*, Yokyakarta, Ar-Ruzz Media.

Hamzah Andi, 1990, *Aspek-aspek Pidana di Bidang Komputer*, Jakarta, Sinar Grafika.

Hamzah Andi. 1993. *Aspek-aspek Pidana di Bidang Komputer*. Jakarta: Sinar Grafika.

Hamzah Andi, 1996, *Ketentuan-Ketentuan Dalam Buku II KUHP Indonesia*, Jakarta

Harry N.P, 2015, *Perlindungan Hukum Terhadap Nasabah Bank Pengguna Fasilitas Internet Banking atas Terjadinya Cyber Crime (Studi Kasus: Bussines Banking Center Mandiri Padang.* Padang.

Indrawan R, Yaniawati R.P, 2014, *Metodologi Penelitian*

Kuantitatif, Kualitatif dan Campuran Untuk Manajemen, Pembangunan, dan Pendidikan, Bandung, Penerbit: PT Refika Aditama.

Karnasudirja, E.D. 1993. *Yurisprudensi Kejahatan Komputer*. Jakarta: Tanjung Agung.

Karnasudirja E.D, 1999, *Bahaya Kejahatan Komputer*, Jakarta

Kian A.M.L, 2015, *Tindak Pidana Credit/Debit Card Fraud dan Penerapan Sanksi Pidananya dalam Hukum Pidana Indonesia*, Papua Barat.

Lexy J. Moleong, 2000, *Metodologi Penelitian Kualitatif*, Bandung: Remaja Rosda Karya.

Mahfud M.D, 2000, *Politik Hukum Nasional*, Bandung.

Maxmanroe, 2018, *Cyber Crime : Pengertian, Jenis dan Metode Kejahatan Cyber Crime*, https://www.maxmanroe.com/vid/teknologi/pengertian-cyber-crime.html, 2 September 2019

Raharjo Agus. 2002. *Cybercrime*. Bandung: Citra Aditya Bakti.

Raharjo Agus, 2003, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PT Citra Aditya Bakti, Bandung.

Rahmah Y.N, 2018, *Pengaruh Penggunaan Internet Banking Dan Perlindungan Nasabah Pengguna Fasilitas Internet Banking Terhadap Cyber Crime Di Daerah*

Istimewa Yogyakarta (Diy), Yogyakarta.

Serambinews, 2014, *Cyber Crime Kejahatan Baru Di Aceh*, https://aceh.tribunnews.com/2014/08/28/cybercrime-kejahatan-baru-di-aceh, 28 Agustus 2019.

Serambinews, 2017, *Ahli Perbankan: BNI Harus Bertanggung Jawab*, https://aceh.tribunnews.com/2017/01/24/ahli-perbankan-bni-harus-bertanggung-jawab, 29 Agustus 2019

Setiawan Deris, 2005, *Sistem Keamanan Komputer*, PT Elex Media Komputindo, Jakarta.

Silalahi H.R.Br, 2012, *Analisis Yuridis Kejahatan Cyber Crime Dalam Pembobolan Mesin ATM Bank*, Surabaya.

Sudarwan Danim, 2002, *Menjadi Peneliti Kualitatif*, Bandung, Pustaka Setia.

Sunggono Bambang, 2005, *Metodologi Penelitian Hukum*, Jakarta, Rajawali Press.

Suryo Roy, 2001, *Kejahatan Cyber di Indonesia*, Kompas

Teknologi.Bisnis, (2016), *Malware: Pengembang dan Penyebar Trojan SpyEye Dihukum Penjara*, https://teknologi.bisnis.com/read/20160421/105/540281/malware-pengembang-penyebar-trojan-spyeye-dihukum-penjara, 29 Agustus 2019

Wahid, Labib, 2010. *Kejahatan Mayantara*. Bandung: Refika Aditama.

Widodo, 2006, *Motivasi Pelaku Cyber Crime Di Indonesia*, Yogyakarta: Aswindo

Widodo. 2011, *Aspek Hukum Kejahatan Mayantara*. Yogyakarta: Aswindo.

DAFTAR LAMPIRAN

Wawancara dengan salah satu petugas Satreskrim di Kapolres Lhokseumawe

Wawancara dengan salah satu pegawai Bank BNI Syariah Lhokseumawe

Bank BNI Syariah Lhokseumawe

DAFTAR WAWANCARA

Wawancara Dengan

Inisial : HN

Jabatan : Non-operasional

Perusahaan : Bank BNI Syariah Lhokseumawe

Tgl/bulan : 10 Januari 2020

Isi Deskripsi Hasil Wawancara

1. L : Kalau boleh tau pak, sejak kapan Bank BNI Syariah ini mulai didirikan ?

   HN : Bank BNI Syariah ini mulai beroperasi sejak 29 April 2000. Pada 19 Juni 2010 status BNI Syariah meningkat menjadi Bank Umum Syariah (BUS).

2. L : Adakah bentuk kejahatan *cyber crime* yang terjadi di Bank BNI Syariah ini?

   HN : Pernah terjadi kasus *cyber crime* yang menyerang 3 Nasabah daan melapor ke Polres Lhokseumawe atas kehilang uang dalam rekeningnya.

3. L : Apa sajakah bentuk kejahatan *cyber crime* yang dialami oleh Bank BNI Syariah ini?

   HN : Dari pengaduan Nasabah atas kehilangan uang mereka dalam rekeningnya, kasus *cyber crime* yang pernah terjadi di Bank BNI Syariah ini adalah kasus *Skimming* dimana uang di rekening Bank

mereka tiba-tiba berkurang.

4. L : Apakah upaya dari pihak Bank BNI Syariah dalam menghadapi kasus *cyber crime* yang marak terjadi di dunia digital saat ini?

HN : Upaya yang bisa diambil dalam penanganan kasus ini di harapkan kepada Nasabah agar tidak bertransaksi *Internet Banking* menggunakan computer di tempat umum, dan selalu memperhatikan notifikasi transaksi pada *Internet Banking* serta tidak mudah memberikan data pribadi berupa token/*user id/*password kepada pihak lain.

Wawancara Dengan

Inisial : ML

Jabatan : Kasat Reskrim

Perusahaan : Kapolres Lhokseumawe

Tgl/bulan : 15 Januari 2020

Isi Deskripsi Hasil Wawancara

1. L : Berhubungan dengan kasus *cyber crime* yang menyerang Nasabah Bank BNI Syariah Lhokseumawe, apakah pelaku kejahatan tersebut berhasil ditangkap?

   ML : Data yang kami peroleh dari dari perkara ini, telah kami periksa 3 pelapor juga telah dimintai keterangan dari penyedia layanan Nasabah BNI, dan sampai sekarang kasus tersebut masih belum bisa ditemukan pelaku tindak kejahatan atas pencurian uang tersebut.

2. L : Apakah ada Tindakan hukum untuk menangani kasus *cyber crime ini*?

   ML : Tindak pidana *cyber crime* di Indonesia telah diatur di dalam Undang-undang *ITE* (Informasi dan Transaksi Elektronik) Nomor 11 Tahun 2008 dan Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008. “UU *ITE* telah menetapkan perbuatan-perbuatan mana

yang termasuk tindak pidana di bidang *cyber crime* dan telah ditentukan unsur-unsur tindak pidana dan penyerangan terhadap berbagai kepentingan hukum dalam bentuk rumusan-rumusan tindak pidana tertentu,"