PERANAN KEPALA SUB DIREKTORAT *CYBER CRIME* DALAM MENANGGULANGI PENIPUAN BERKEDOK INVESTASI *ONLINE* DI KEPOLISIAN DAERAH BALI

Drs. I Gede Sujana, M.H
Dwijendra University, Denpasar, Bali
e-mail: dalungsujana@gmail.com

Abstrak:

Tujuan dari penelitian ini adalah untuk mengetahui Bagaimana Peranan Kepala Sub Direktorat *Cyber Crime* Dalam Menanggulangi Penipuan Berkedok Investasi *Online* di Kepolisian Daerah Bali. Disamping itu untuk mengetahui faktor yang menghambat Kepala Sub Direktorat *Cyber Crime* Dalam Menanggulangi Penipuan Berkedok Investasi *Online* di Kepolisian Daerah Bali.

Jenis penelitian ini adalah penelitian deskriptif dengan menggunakan pendekatan kualitatif. Teknik pengumpulan data yang digunakan yaitu wawancara dan dokumentasi. Teknik analisis data yang diguanakan dalam penelitian ini adalah analisis data induktif, melalui reduksi data, unitisasi/kategorisasi data, dan penarikan simpulan.

Dari hasil penelitian menunjukan bahwa,1) Bagaiamana Peranan Kepala Sub Direktorat *Cyber Crime* Dalam Menanggulangi Penipuan Berkedok Investasi *Online* di Kepolisian Daerah Bali yaitu: dengan cara menerima laporan atau pengaduan dari masyarakat atau dengan melakukan *cyber* parpol guna menemukan pelaku dengan cara penyelidikan kemudian penyidikan.2) Hambatan Kepala Sub Direktorat *Cyber Crime* Dalam Menanggulangi Penipuan Berkedok Investasi *Online* di Kepolisian Daerah Bali adalah faktor *hadware* atau *software* yang kurang memadai untuk melakukan penyidikan, anggaran, kemampuan penyidik, alat bukti, kesadaran hukum untuk melaporkan kasus ke kepolisian masih sangat rendah, perangkat hukum yang belum memadai dan fasilitas komputer forensik yang belum memadai.

Berdasarkan penelitian dan pembahasan tentang Peranan Kepala Sub Direktorat *Cyber Crime* Dalam Menanggulangi Penipuan Berkedok Investasi *Online* di Kepolisian Daerah Bali dapat disimpulkan bahwa *cyber crime* merupakan perbuatan yang merugikan. Modus operandi *cyber crime* sangat beragam dan terus berkembang sejalan dengan perkembangan teknologi, tetapi jika diperhatikan lebih saksama akan terlihat bahwa banyak di antara kegiatan-kegiatan tersebut memiliki sifat yang sama dengan kejahatan-kejahatan konvensional. Perbedaan umumnya adalah bahwa *cyber crime* melibatkan komputer dalam pelaksanaanya. Sistem perundang-undangan di Indonesia belum mengatur secara khusus mengenai kejahatan komputer melalui media internet. Beberapa peraturan yang ada baik yang terdapat di dalam KUHP maupun diluar KUHP untuk sementara dapat diterapkan terhadap beberapa kejahatan, tetapi ada juga kejahatan yang tidak dapat diantisipasi oleh undang-undang yang saat ini berlaku.
Kata Kunci : *Cyber Crime*, penipuan, Investasi *Online.*

THE ROLE OF THE HEAD OF SUB DIRECTORATE CYBER CRIME IN DETERMINING ONLINE INVESTMENT MARKETING DECADES IN REGIONAL POLICE BALI

Drs. I Gede Sujana, M.H
Dwijendra University, Denpasar, Bali
e-mail: dalungsujana@gmail.com

Abstract:

The purpose of this study is to find out how the role of the Head of Sub Directorate of Cyber Crime in Overcoming Fraud under the Fraudulent Online Investment in the Regional Police Bali. Besides, to know the factors that inhibit the Head of Sub Directorate of Cyber Crime in Tackling Fraud under the Fraudulent Online Investment in the Bali Regional Police. The type of this research is descriptive research using qualitative approach. Data collection techniques used are interviews and documentation. Data analysis technique used in this research is inductive data analysis, through data reduction, unitization / data categorization, and conclusion drawing.

The results of the research show that 1) how the role of the Head of Sub Directorate of Cyber Crime in Tackling Fraud under the Online Investment in the Bali Regional Police is by receiving reports or complaints from the public or by conducting cyber parties to find the perpetrators by means of investigation and then investigation.2) Obstacles Head of Sub Directorate of Cyber Crime in Overcoming Fraud Under the False of Online Investment in Bali Regional Police is a factor of hadware or software that is inadequate to conduct investigation, budget, investigator ability, evidence, law awareness to report case to police still very low, which has not been sufficient and inadequate computer forensic facilities.

Based on research and discussion about the role of Head of Sub Directorate of Cyber Crime In Overcoming Fraud Under the False Investment Online in Bali Regional Police can be concluded that cyber crime is a harmful action. The modus operandi of cyber crime varies greatly and continues to grow in line with technological developments, but if more careful attention will be observed that many of these activities have the same characteristics as conventional crimes. The general difference is that cyber crime involves a computer in its implementation. The Indonesian legislation system has not specifically regulated computer crimes through internet media. Some of the existing rules contained within the Criminal Code as well as outside the Criminal Code are temporarily applicable to some crimes, but there are also crimes that can not be anticipated by current laws.

Keywords: Cyber Crime, scams, Online Investment.

I. PENDAHULUAN

Fenomena pesatnya perkembangan teknologi informasi telah merebak di seluruh belahan dunia. Tidak hanya negara maju saja, namun negara berkembang juga telah memacu perkembangan teknologi informasi pada masyarakatnya masing-masing. Sehingga teknologi informasi mendapatkan kedudukan yang penting bagi kemajuan sebuah bangsa. Seiring dengan perkembangan kebutuhan masyarakat di dunia, teknologi informasi (*information technology*) memegang peran penting, baik di masa kini maupun di masa mendatang. Teknologi informasi di yakini membawa keuntungan dan kepentingan yang besar bagi negara-negara di dunia. Dengan demikian, teknologi informasi telah berhasil memicu dan memacu perubahan tatanan kebutuhan hidup masyarakat dibidang sosial dan ekonomi, yang *notabene* sebelumnya bertransaksi ataupun bersosialisasi secara konvesional menuju transaksi ataupun sosialisasi secara elektronik.

Internet merupakan bukti dari perkembangan teknologi komunikasi dan informasi, yang dalam sejarahnya berkembang dengan sangat pesat dan telah menciptakan dunia baru yang disebut dengan istilah *cyber space*. Pengertian dari *Cyber space*, adalah sebuah dunia komunikasi berbasis komputer (*computer mediated communication*) ini menawarkan realitas yang baru, yaitu realitas virtual (*virtual reality*). Dengan terciptanya realitas virtual dari penggunaan internet tersebut, pengguna dimanjakan untuk menjelajahi atau menelusuri dunia *cyber space* dengan menembus batas kedaulatan suatu negara, batas budaya, batas agama, batas geografis, politik, ras, hirarki, birokasi dan sebagainya . Dengan berkembangnya internet, semakin banyak orang menikmati realitas baru yang ditawarkan.

Secara umum, dampak positif dari pengguna internet yaitu kemudahan komunikasi dengan siapapun di seluruh dunia;sebagai media pertukaran data dengan menggunakan fasilitas *search engine* yang memudahkan pengguna di seluruh dunia dapat bertukar informasi dengan cepat, murah, penting dan akurat sehingga manusia dapat mengetahui apa saja yang terjadi; digunakan sebagai lahan informasi untuk bidang pendidikan, kebudayaan dan lain-lain; serta kemudahan bertransaksi dan berbisnis di tempat dalam bidang perdagangan. telah dijelaskan di depan bahwa dengan semakin muktahirnya teknologi dan perkembangan fasilitas internet, semua orang dapat dengan mudah menggunakan dan menikmati setiap hal yang disajikan di internet. Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia secara global.

Disamping telah menyebabkan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat seperti pergeseran nilai sosial masyarakat dan cenderung menciptakan kepribadian yang individualitas, juga sekaligus membuka peluang besar bagi terjadinya tindak kejahatan melalui penggunaan dunia siber/maya *(cyber crime*). Dengan terjadinya perbuatan-perbuatan melawan hukum tersebut, maka ruang lingkup hukum harus diperluas untuk menjangkau perbuatan-perbuatan tersebut, seperti tindak manipulasi data, *hacking* dan tindak penipuan yang menggunakan fasilitas-fasilitas di internet (Abdul Wahid dan Mohammad Labib, 2005 : 23)

Salah satu regulasi internasional yang mengatur mengenai *cyber crime* yaitu *European Union Convention On Cyber crime* atau biasa dikenal Konvensi Budupest tahun 2001, merupakan aturan mengenai *cyber crime* yang dibentuk oleh organisasi

internasional yaitu *Council Of Europe* (Negara-negara yang tergabung dalam uni eropa), yang secara jelas mengatur bentuk-bentuk *cyber crime* dan kewajiban negara-negara peratifikasi dalam penanganan *cyber crime* secara nasional maupun internasional. Indonesia sendiri telah memiliki Undang-undang khusus mengenai transaksi yang berbasis elektronik yaitu undang-undang Nomor 11 tahun 2008 tentang informasi dan transaksi Elektronik. Namun yang menjadi "dilema" regulasi saat ini bahwa apakah aturan-aturan tersebut, baik tingkat nasional maupun internasional mampu menjangkau dan mengikuti kemajuan dan pola perubahan *cyber crime* itu sendiri seiring dengan kian pesatnya perkembangan kecanggihan teknologi berinternet hingga saat ini.

Dengan segala kemudahan yang diberikan di dunia siber/maya maka semakin besar pula kemudahan untuk melakukan *cyber crime.* Perkembangan yang pesat dalam teknologi internet menyebabkan kejahatan baru di bidang itu juga muncul (Budi Suhariyanto, 2012: 3). Saat ini, berbagai macam bentuk *cyber crime* berkembang di masyarakat, misalnya kejahatan manipulasi data, *spionase, sabotase,* provokasi, *money laundering,* penipuan secara *online, hacking, hoax* dan berbagai macam lainnya. Salah satu bentuk *cyber crime* yang saat ini berkembang dan bervariasi modus kejahatan serta sedang marak terjadi di masyarakat pengguna internet yaitu praktik penipuan online di internet dengan menggunakan media sosial. Media sosial (*social media*) sebagai media komunikasi yang saat ini sedang diminati oleh hampir seluruh pengguna internet atau *nitizen* menjadi salah satu sarana melakukan penipuan internet ini.

Bali sebagai daerah pariwisata mengalami pertumbuhan jumlah wisatawan mancanegara yang cukup signifikan maka akan memberikan dampak positif dan negatif, salah satu dampak positif adalah meningkatkan devisa negara namun disisi lain dapat menimbulkan dampak negatif bagi industri pariwisata, salah satu contoh dampak negatifnya yaitu maraknya *online travel agent* (OTA) China yang telah membuka kantor dan mengaji orang local dan menjual paket wisata dengan harga yang tidak masuk akal. Dengan begitu maraknya kasus penipuan berkedok investasi *online* maka penulis tertarik untuk melakukan penelitian yang berjudul " Peranan Kepala Sub Direktorat *Cyber Crime* Dalam Menanggulangi Penipuan Berkedok Investasi *Online* di Kepolisian Daerah Bali "

Berdasarkan latar belakang di atas maka penulis merumuskan permasalahan sebagai berikut : Bagaimana peranan Kepala Sub Direktorat *Cyber Crime* Dalam Menanggulangi Penipuan Berkedok Investasi *Online* di Kepolisian Daerah Bali? Tujuan yang ingin dicapai dalam penelitian ini adalah untuk mengetahui peranan Kepala Sub Direktorat *Cyber Crime* dalam menanggulangi penipuan berkedok investasi *online* serta faktor yang menghambatnya. Hasil penelitian diharapkan dapat memberikan informasi dalam pemanfaatan internet bagi masyarakat secara nasional maupun internasional untuk memahami bentuk penipuan berkedok investasi *online* dan cara pencegahan praktik penipuan internet (*Internet Fraud*) sebagai bentuk *cyber crime* khususnya di Kepolisian Daerah Bali.

Istilah dan Defenisi *Cyber crime*

Tentang definisi *cyber crime*,terdapat beberapa versi penggunaan istilah dan pengertian *cyber crime* itu sendiri. Dalam beberapa kepustakaan, *cyber crime* sering diidentikan sebagai *computer crime* (Gamble,Teri and Michael: 47). Menurut *U.S Departement of Justice, computer crime sebagai: "Any illegal act requiring knowledge of computer technology for its*

perpetration,investigation or presecution (Maskun 2013: 47).Namun beberapa ahli memberi perbedaan antara *cyber crime* dengan *computer crime*.*Cyber crime* dan *computer crime* merupakan dua istilah yang berbeda sebagaimana yang dikatakan oleh Nazura Abdul Manap, (2001: 3) sebagai berikut "*Defined broadly, "computer crime" could reasonably include a wide variety of criminal offences, activities or issues. It also known as a crime commited using a computer as a tool and it involves direct contact between the criminal and the computer. For instance, a dishonest bank clerk who unauthorisedly transfers a customer's money to a dormant account for his own interest or a person without permission has obtained acces to other person's computer confidential. These situations require direct access by a hacker to the victim's computer. There is no internet line involved, or only limited networking used such as the Local Area Network (LAN)." Whereas, cyber crime are crime commited virtually thourgh internet online. This means that the crimes could extend to other countries, which is beyond the Malaysian jurisdiction. Anyway, it causes no harm to refer computer crimes as cyber crimes or vice versa, since they have same impact in law*.

Sejarah dan ruang lingkup *Cyber crime*

Cyber crime terjadi bermula dari kegiatan *hacking* yang telah ada lebih dari satu abad. Pada tahun 1870-an, beberapa remaja telah merusak sistem telepon baru Negara dengan merubah otoritas. Berikut akan ditunjukan seberapa sibuknya para *hacker* telah ada selama 35 tahun terakhir. Awal 1960 fasilitas universitas dengan kerangka utama komputer yang besar, seperti laboratorium kepintaran buatan (arti *ficial intel ligence*) MIT, menjadi tahap percobaan bagi para *hacker*. Pada awalnya, kata " *hacker*" berarti positif untuk seorang yang menguasai komputer yang dapat membuat sebuah program melebihi apa yang dirancang untuk melakukan tugasnya. Awal 1970 John Draper membuat sebuah panggilan telepon jarak jauh secara gratis dengan meniupkan nada yang tepat ke dalam telepon yang memberitahukan kepada sistem telepon agar membuka saluran. Draper menemukan siulan sebagai hadiah gratis dalam sebuah kotak sereal anak-anak. Draper, yang kemudian memperoleh julukan "Captain crunch" ditangkap berulangkali untuk pengerusakan telepon pada tahun 1970-an . pergerakan social Yippie memulai majalah YIPL/TAP (*Youth International Party Line/ Technical Assistance Program*) untuk menolong para *hacker* telepon (disebut "*phreaks*") membuat panggilan jarak jauh secara gratis. Dua anggota dari *California's Homebrew Computer Club* memulai membuat "*blue boxes*" alat yang digunakan untuk meng-*hack* ke dalam sistem telepon. Para anggotanya, yang mengadopsi pegangan "*Berkeley Blue" (Steve Jobs)* dan "*Oak Toebark" (Steve Wozniak*), yang selanjutnya mendirikan *Apple computer*. Awal 1980 pengarang William Gibson memasukkan istilah "*Cyber Space*" dalam sebuah novel fiksi ilmiah yang disebut *Neurimancer*. Dalam satu penangkapan pertama dari para *hacker*, FBI menggerebek markas 414 di Milwaukee (dinamakan sesuai kode area local) setelah para anggotanya menyebabkan pembobolan 60 komputer berjarak dari *memorial Sloan-Kettering Cancer Center ke Los Alamos National Laboratory. Comprehensive Criem Contmrol Act* memberikan yuridiksi *Secret Service* lewat kartu kredit dan penipuan Komputer. Dua bentuk kelompok *hacker, the legion of doom* di amerika serikat dan *the chaos computer club* di Jerman. Akhir 1980 penipuan komputer dan tindakan penyalahgunaan memberi kekuatan lebih bagi otoritas *federal computer emergency response team* dibentuk oleh agen

pertahanan Amerika Serikat bermarkas pada *Carnegie mellon university di pitt sburgh*, misinya untuk menginvestigasi perkembangan volume dari penyerangan pada jaringan komputer pada usianya yang ke 25, seorang *hacker* veteran bernama Kevin mitnick secara rahasia memonitor *email* dari MCI dan pegawai keamanan digital *equipment*. Dia dihukum karena merusak komputer dan mencuri *software* dan hal itu dinyatakan hukum selama satu tahun penjara. Pada oktober 2008 muncul sesuatu virus baru yang bernama *conficker* (juga disebut *downup downandup* dan kido) yang terkatagori sebagai virus jenis *worm.conficker* menyerang *windows* dan paling banyak ditemui dalam *windows XP.microsoft* merilis *patch* untuk menghentikan *worm* ini pada tanggal 15 oktober 2008. Heinz haise memperkirakan *conficker* telah menginfeksi 2.5 juta PC pada 15 januari 2009, sementara The Guardian memperkiran 3.5 juta PC terinfeksi. Pada 16 januari 2009, *worm* ini telah menginfeksi hampir 9 juta PC,menjadikannya salah satu infeksi yang paling cepat menyebar dalam waktu singkat.

Sesuai sifat global internet, ruang lingkup kejahatan ini juga bersifat global.*Cyber crime* sering kali dilakukan secara transnasional, meliputi batas negara sehingga sulit dipastikan yurisdiksi hukum negara mana yang berlaku terhadap pelaku.(Akbar Kurnia Putra 2014: 99). Dalam perkrmbangannya, lingkup cakup kejahatan dunia maya meliputi: (a) pembajakan; (b) penipuan; (c) pencurian; (d) pornografi; (e) pelecehan; (f) penfitnahan; dan (g) pemalsuan (Maskun, 201 3: 51).

Bentuk dan Jenis *Cyber Crime*

Sesungguhnya banyak perbedaan di antara para ahli dalam mengklasifikasikan kejahatan komputer (*computer crime*). Ternyata dari klasifikasi tersebut terdapat kesamaan dalam beberapa hal. Untuk memudahkan klasifikasi kejahatan komputer (*computer crime)* tersebut, maka dari beberapa klasifikasi dapat disimpulkan:

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-kepentingan yang tidak sesuai dengan tujuan pengelolaan atau operasinya.
4) Tindakan-tindakan yang mengganggu operasi komputer.
5) Tindakan merusak peralatan komputer atau peralatan yang berhubungan dengan komputer atau sarana penunjangnya.

Kejahatan yang berhubungan erat dengan penggunaan tekonologi berbasis Komputer dan jaringan telekomunikasi dalam beberapa literatur dan praktiknya dikelompokan dalam beberapa bentuk antara lain (Maskun, 2013 : 51)

1).*Unauthorized access to computer system and service*, yaitu kejahatan yang dilakuakan dalam salah suatu sistem jaringan komputer secara tidak sah, tanpa ijin, atau tanpa pengetahuan dari pemilik sistem jaringan komputer yan dimasukinya. 2).*Illegal Contents*, yaitu kejahatan dengan memasukan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban umum. 3). *Data Forgery*, yaitu kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melaui internet. 4).*Cyber Espinoge*, yaitu kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan Komputer (*Computer network system*) pihak sasaran. 5). *Cyber sabotage and Extortion*, yaitu kejahatan yang dilakukan membuat program, perusakan

atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung ke internet. Kejahatan ini kadang disebut dengan *cyber terrorism*. 6).*Offence Againts intellectual property*. Kejahatan yang ditujukan terhadap HAKI (Hak Atas Kekayaan Intelektual) yang dimiliki pihak lain di internet. 7). *Infringements of privacy*. Kejahatan ini ditujukan terhadap informasi seseseoang yang merupakan hal yang sangat pribadi dan rahasia.

Jenis-jenis *cyber crime* berdasarkan motifnya dapat terbagi dalam beberapa hal :

1) *Cyber crime* sebagai tindakan kejahatan murni
2) *Cyber crime* sebagai tindakan kejahatan abu-abu
3) *Cyber crime* menyerang individu
4) *Cyber crime* yang menyerang hak cipta (hak milik)
5) *Cyber crime* yang menyerang pemerintah

Makna dari penipuan berkedok investasi melalui sistem *online* adalah perbuatan atau cara penipuan dengan memakai kedok atau melakukan sesuatu sebagai penutup keadaan sebenarnya, menggunakan sesuatu sebagai alat untuk menutup diri yang dalam hal ini penipuan diwujudkan dalam penawaran usaha berupa penanaman uang atau modal disuatu perusahan atau proyek dengan metode menggunakan jarinagan internet untuk tujuan memperoleh keuntungan yang sebenarnya perusahan tersebut fiktif atau tidak kredibel dan tidak dapat di pertanggungjawabkan atau dengan kata lain tujuan utama adalah menipu tetapi ditutupi dengan kegiatan/ usaha investasi.

II. METODE PENELITIAN

Jenis penelitian ini adalah penelitian kualitatif dengan menggunakan pendekatan empiris. Penelitian kualitatif dapat diartikan sebagai prosedur pemecahan masalah yang diselidiki dengan menggambarkan/melukiskan keadaan subjek/objek penelitian (seseorang, lembaga,masyarakat dan lain-lain), pada saat sekarang berdasarkan fakta-fakta yang nampak atau sebagai mana adanya (Hadari Nawawi, 2001:63). Penelitian kualitatif adalah penelitian yang bertujuan membuat, melukiskan, menggambarkan situasi-situasi atau kejadian-kejadian (Sumandi Suryabrata, 2005:18). Penelitian ini bersifat menjelaskan, menggambarkan atau mendeskripsikan peranan yang Kepala Sub Direktorat *CyberCrime* Dalam Menanggulangi Penipuan Berkedok Investasi Melalui Sistem *Online* di Kepolisian Daerah Bali.

Sumber Data

Menurut Arikunto (2010: 82) data adalah “hasil penelitian pencatatan peneliti baik berupa fakta maupun angka-angka” dengan demikian tidak semua yang dinamakan informasi atau keterangan disebut data, demikian data yang dimaksud dalam penelitian ini adalah informasi yang tidak ada hubungannya dengan penelitian, jadi informasi yang tidak ada hubungannya dengan penelitian yang dilakukan bukan termasuk data.

1) Data Primer
   Menurut Umar Husein (2003: 56), data primer merupakan data yang diperoleh langsung dilapangan oleh peneliti sebagai obyek penulisan. Jenis data ini meliputi informasi dan keterangan mengenai Peranan Kepala Sub Direktorat *Cyber Crime* Dalam Menanggulangi Penipuan Berkedok Investasi *Online* diKepolisian Daerah Bali.
2) Data sekunder
   Soemitro (1990: 52) juga menyatakan bahwa data sekunder “merupakan data yang diperoleh melalui studi pustaka”. Dalam penelitian ini untuk mendapatkan data sekunder penulis melakukan studi/penelitian kepustakaan guna untuk

memperoleh landasan teoritis yang bersumber pada buku literatur yang berkaitan dengan penelitian.

Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini yaitu:

1) Wawancara
   Teknik wawancara yang digunakan dalam penelitian ini adalah wawancara tidak terstruktur dimana peneliti tidak menggunakan pedoman wawancara yang telah tersusun secara sistematis dan lengkap, pedoman wawancara hanya berupa garis besar permasalahan yang ditanyakan (Sugiyono, 2010:233-234).
2) Dokumentasi
   Teknik pengumpulan data dengan dokumentasi adalah pengambilan data yang diperoleh melalui dokumen-dokumen (Husaini Usman dan Purnomo Setiady Akbar, 1996:73).

Teknik Analisis Data

Teknik analisis data yang digunakan dalam penelitian ini adalah analisis data induktif. Analisis data induktif yaitu penarikan kesimpulan yang berangkat dari fakta yang khusus, peristiwa yang konkrit kemudian ditarik kesimpulan secara umum dengan menyajikan data dan menganalisis data dalam bentuk deskriptif. Langkah-langkah analisis yang digunakan dalam penelitian ini analisis data kualitatif, yang menurut Sayekti Pujosuwarno (1992:19) meliputi:

1) Reduksi Data
   Reduksi data merupakan proses pemilihan pemusatan perhatian dan pengabstraksian dan pentransfrormasian data kasar dari lapangan. Data yang di hasilkan dalam proses wawancara dan dokumentasi merupakan data yang masih kompleks dan kasar sehingga peneliti perlu untuk melakukan pemilihan data yang relavan dan bermakna yang dapat digunakan dengan memilih data pokok yang mengarah pada permasalahan penelitian.
2) Unitisasi dan Kategori Data
   Data yang diperoleh dari wawancara dan dokumentasi akan disederhanakan dan dipilih, kemudian disusun secara sistematis ke dalam kategori dengan sifat masing-masing data yang spesifik sesuai dengan tujuan penelitian yang sifatnya urgen dan pokok, sehingga data dapat memberikan gambaran penelitian yang jelas.
3) Penarikan Kesimpulan
   Data yang telah di interprestasikan secara sistematis tersebut kemudian diperoleh kesimpulan. Pengambilan kesimpulan dilakukan dengan cara berfikir induktif yaitu dari hal-hal yang khusus diarahkan kepada hal-hal yang umum untuk mengetahui tentang Peranan Kepala Sub Direktorat *Cyber Crime* Dalam Menanggulangi Penipuan Berkedok Investasi *Online* di Kepolisian Daerah Bali.

III. HASIL PENELITIAN DAN PEMBAHASAN

Peranan Kepala Sub Direktorat *Cyber Crime* Dalam Menanggulangi Penipuan Berkedok Investasi Online Dikepolisian Daerah Bali

Berdasarkan hasil wawancara, diketahui bahwa memang penting Peranan Kepala Sub Direktorat *Cyber Crime* Dalam Menanggulangi Penipuan Berkedok Investasi *Online* di Kepolisian Daerah Bali. Hal ini dapat dibuktikan dari hasil wawancara dengan Bapak Andi Prasetyo,SH pada tanggal 23 Maret 2018 bahwa peranan Kepala Sub Direktorat *Cyber Crime* di Kepolisian Daerah Bali yaitu dengan cara menerima laporan atau pengaduan dari masyarakat atau dengan melakukan *Cyber*

Partol guna menemukan pelaku dengan cara penyidikan secara digital investigasi.

Untuk memperoleh gambaran yang jelas mengenai Peranan Kepala Sub Direktorat *Cyber Crime* Dalam Menanggulangi Penipuan Berkedok Investasi *Online* di Kepolisian Daerah Bali akan di uraikan sebagai berikut :

1. Penyelidikan

Penyelidikan terhadap kasus penipuan berkedok investasi online di kepolisian daerah bali dilakukan oleh Polisi Penyelidik Unit B bidang *Fismondev* Subdit I/Ekonomi Ditreskrimsus Polda Bali. Sebelum dilakukan tindakan penyidikan, dilakukan dulu penyelidikan oleh pejabat penyelidik, dengan maksud dan tujuan mengumpulkan bukti permulaan atau bukti yang cukup agar dapat dilakukan tindak lanjut penyidikan. Setelah mendapatkan laporan adanya penipuan berkedok investasi melalui sistem *online* dilakukan tindakan penyelidikan. Pada tahap penyelidikan, polisi penyelidik melakukan serangkaian tindakan yaitu:

a). Menerima laporan atau pengaduan dari seseorang tentang adanya penipuan berkedok investasi melalui sistem *online.* Sentral Pelayanan Kepolisian Terpadu (SPKT) Kepolisian Daerah Bali menerima laporan atau pengaduan dari masyarakat tentang telah atau sedang atau diduga akan terjadi peristiwa dalam hal ini penipuan berkedok investasi *online*. Petugas SPKT mencatat semua hal yang dilaporkan. Laporan polisi yang telah dicatat tersebut disampaikan kepada Bagian Pembinaan Operasional (Bagbinopsnal) Ditreskrimsus Polda Bali untuk selanjutnya dilakukan analisa terhadap laporan yang masuk dan kemudian menunjuk salah satu subdit yang berwenang untuk menangi kasus tersebut, dalam hal ini subdit I/Ekonomi. Kasubdit I/Ekonomi kemudian menunjuk salah unit yang berwenang untuk menangani kasus tersebut, dalam hal ini unit B bidang *Fismondev* Subdit I/Ekonomi Ditreskrimsus Polda Bali untuk mulai menindak dan melakukan pemeriksaan setelah administrasi penyelidikan berupa Surat Perintah Tugas dan Surat Perintah Penyelidikan Lengkap.

b). Mencari keterangan dan alat bukti. Dalam mencari keterangan dan alat bukti kasus penipuan berkedok investasi *online*, penyelidik melakukan pemanggilan dan pemeriksaan terhadap saksi pelapor atau korban serta penyamaran maupun *"under cover"* (penyusupan). Pemanggilan dan pemeriksaan terhadap saksi pelapor atau korban dilakukan guna mendapatkan keterangan tentang peristiwa yang diduga. Penyamaran yaitu penyelidik menjadi seolah-olah bagian dari area yang diduga terjadi kasus penipuan *online* dan mengganti identitas sesuai dengan keadaan area tersebut guna mendapatkan keterangan dan alat bukti. Penyamaran dilakukan polisi penyelidik dengan berpura-pura akan menjadi *investor* pada sebuah perusahaan atau individu penawar investasi. Penyusupan disini yaitu penyelidik memasuki area yang diduga sebagai tempat terjadinya kasus penipuan *online* secara sembunyi-sembunyi untuk tidak diketahui siapapun guna mendapatkan keterangan dan alat bukti.

c). Kewenangan penyelidik membuat dan menyampaikan laporan hasil pelaksanaan tindakan penyelidikan. Penyelidik wajib membuat dan menyampaikan laporan tertulis hasil pelaksanaan tindakan penyelidikan demi untuk mempertanggungjawaban dan pembinaan pengawasan terhadap penyelidik kasus penipuan berkedok

investasi *online*, sehingga tindakan yang dilakukan penyelidik berupa pemanggilan serta pemeriksaan terhadap pelapor maupun saksi dan pengumpulan bahan keterangan dari sebuah perusahaan atau individu penawar investasi tertera dalam laporan hasil pelaksanaan tindakan penyelidikan tersebut. Setelah terkumpul cukup bukti pada tahap penyelidikan kasus penipuan berkedok investasi *online* yaitu minimal dua alat bukti yakni keterangan saksi (pelapor) atau korban dan petunjuk dilakukan penyidikan.

2. Penyidikan

Penyidikan merupakan serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang untuk mencari serta mengumpulkan bukti yang terjadi dan guna menemukan tersangkanya (Pasal 1 angka 2 KUHP). Dalam hal ini penyidikan dilakukan oleh polisi penyidik unit B bidang Fismondev Subdit I/ Ekonomi Ditreskrimsus Kepolisian Daerah Bali. Setelah dikeluarkan surat perintah penyidikan dan surat perintah tugas, polisi penyidik segera melakukan penyidikan terhadap pelaku kejahatan penipuan berkedok investasi online dikepolisian daerah Bali. Adapun tindakan penyidikan yang dilakukan oleh polisi penyidik Unit B bidang Fiskal Moneter (*Fismondev*) Subdit I/ Ekonomi Ditreskrimsus Kepolisian Daerah Bali diuraikan sebagai berikut:

a).Penangkapan

Penangkapan ini dilakukan untuk kepentingan penyidikan dengan ketentuan Pasal 16 ayat (2) KUHAP yang berbunyi untuk kepentingan penyidikan, penyidik dan penyidik pembantu berwenang melakukan penangkapan. Polisi Penyidik Unit B bidang *Fismondev* Subdit I/ Ekonomi Ditreskrimsus Kepolisian Daerah Bali dalam melakukan penangkapan berdasarkan alasan seorang tersangka diduga keras melakukan tindak pidana dan dugaan yang kuat itu didasarkan pada bukti permulaan yang cukup. Penangkapan tersebut dilakukan oleh beberapa orang petugas dari Unit B bidang *Fismondev* Subdit I/ Ekonomi Ditrekrimsus Kepolisian Daerah Bali yang telah ditunjuk oleh Direktur Reserse Kriminal Khusus (Dirreskrimsus). Dalam melakukan penangkapan terhadap tersangka polisi penyidik harus membawa surat tugas. Selain itu polisi penyidik Unit B *Fismondev* Subdit I/ Ekonomi Ditreskrimsus Kepolisian Daerah Bali harus memperlihatkan surat perintah penangkapan dari Direktur Reserse Kriminal Khusus (Dirreskrimsus) yang berisi identitas tersangka, alasan penangkapan, uraian singkat perkara kejahatan dan tempat tersangka diperiksa. Penangkapan dilakukan karena berdasarkan keterangan saksi-saksi, serta bukti-bukti yang ada dan di duga kuat telah melakukan tindak pidana sebagaimana dimaksud dalam Pasal 378 KUHP, kemudian tersangka dibawa kekantor Direktorat Reserse Kriminal Khusus Kepolisian Daearah Bali guna penyidikan lebih lanjut. Atas penangkapan tersangka, kemudian dibuatkan Berita Acara Penangkapan.

1) Penahanan

Untuk kepentingan penyidikan dan berdasarkan hasil pemeriksaan diperoleh bukti yang cukup, tersangka diduga keras melakukan tindak pidana penipuan sebagaimana diatur dalam Pasal 378 KUHP yang dapat dikenakan penahanan, Penahanan tersebut dilakukan oleh beberapa orang petugas dari Unit B bidang *Fismondev* Subdit I/ Ekonomi Ditrekrimsus Kepolisian Daerah Bali yang telah diperintahkan oleh Direktur Reserse Kriminal Khusus. Atas penahanan tersebut kemudian dibuatkan berita acara penahanan.

2) Pengeledahan

Pengeledahan bertujuan untuk mencari dan mengumpulkan fakta dan bukti serta dimaksudkan untuk mendapatkan orang yang diduga keras sebagai tersangka pelaku. dalam kasus tindakan penipuan berkedok investasi *online*, untuk kepentingan penyidikan, penyidik unit B bidang *Fismondev* subdit I/ Ekonomi Kepolisian Daerah Bali dapat melakukan penggeledahan rumah atau penggeledahan pakaian atau penggeledahan badan menurut tata cara yang ditentukan dalam KUHAP (Pasal 32 KUHAP). Dalam melakukan penggeledahan rumah, penyidik unit B bidang *Fismondev* subdit I/Ekonomi Kepolisian Daerah Bali harus memenuhi syarat yaitu dengan surat ijin ketua pengadilan negeri setempat penyidik dalam melakukan penyidikan dapat mengadakan penggeledahn rumah yang diperlukan; dalam hal yang diperlukan atas perintah tertulis dari penyidik, petugas kepolisian dapat memasuki rumah, setiap kali memasuki rumah harus disaksikan oleh kepala desa, ketua lingkungan dan dua orang saksi, dalam hal tersangka atau penghuni menolak atau tidak hadir, dalam waktu dua hari setelah memasuki dan atau menggeledah rumah, harus dibuat suatu berita acara dan turunannya disampaikan kepada pemilik atau penguhi rumah bersangkutan (Pasal 33 (ayat 1 – 5) KUHAP).

3) Penyitaan

Polisi penyidik unit B bidang *Fismondev* Subdit I/Ekonomi Ditreskrimsus Kepolisian Daerah Bali selain melakukan penahanan terhadap tersangka penyidik juga melakuan penyitaan terhadap barang bukti. Penyitaan hanya dapat dilakukan oleh penyidik dengan surat ijin ketua pengadilan negeri setempat (pasal 38 ayat (1) KUHAP). Penyitaan oleh penyidik unit B bidang *Fismondev* subdit I/Ekonomi Ditreskrimsus Kepoilisian Daerah Bali dilakuan denga terlebih dahulu menunjukan tanda pengenal sesuai dengan ketentuan pasal 128 KUHAP. Setelah melakukan penggeledahan dengan disaksikan oleh kepala desa atau kepala lingkungan dan dua orang saksi (pasal 129 ayat (1) KUHAP). Penyidik unit B bidang *Fismondev* subdit I/Ekonomi Ditreskrimsus Kepolisian Daerah Bali membuat berita acara yang dibacakan, ditandatangani serta salinannya disampaiakn kepada atasan penyidik, orang yang disita, keluaraganya dan kepala desa. Benda-benda yang dikenai penyitaan disimpan dalam rumah penyimpanan di Kepolisian Daerah Bali.

4) Pemanggilan

Demi untuk melakukan pemeriksaan, penyidik unit B bidang *Fismondev* subdit I/Ekonomi Ditreskrimsus Kepolisian Daerah Bali melalkuan pemanggilan terhadap saksi yang dianggap perlu untuk diperiksa. Pemanggilan saksi dilakukan penyidik dengan berhati-hati dan teliti. Jangan sampai ada saksi yang dipanggil, ternyata tidak dapat memberikan keterangan apapun. Untuk memanggil dan menjadikan seseorang untuk diperiksa sebagai saksi, pejabat atau penyidik pembantu harus benar-benar berpedoman pada kriteria yang ditentukan oleh pasal I butir 26 KUHAP, yaitu seseorang yang mendengar sendiri, melihat sendiri, mengalami sendiri peristiwa pidananya, dan orang yang bersangkutan apa yang ia dengar, ia lihat serta ia alami. Guna kepentingan penyidikan, selain melakukan pemanggilan terhadap saksi-saksi, polisi penyidik mendatangkan ahli dari badan pengawasan perdagangan berjangka komoditi, auditor dari akuntan publik dan ahli IT. Dalam kasus penipuan berkedok investasi online, pemanggilan saksi

dialkukan dengan panggilan berbentuk surat panggilan.

5) Pemeriksaan
   Pemeriksaan penyidikan dilakukan oleh polisi unit B bidang *Fismondev* subdit I/Ekonomi Ditreskrimsus Kepolisian Daerah Bali. Pemeriksaan penyidikan dilakukan terhadap tersangaka yang karena perbuatan/kedaan berdasarakan bukti permulaan yaitu keterangan saksi (pelapor) dan bukti petunjuk, patut diduga sebagai pelaku tinfak pidana, terhadap saksi yang dianggap perlu untuk diperiksa dan ahli yang diperlukan dalam hubungannya dengan pemeriksaan perkara karena pada kasus penipuan berkedok investasi online sangat perlu dilakukan karena tindak pidana ini melibatkan ilmu dan teknologi yang terus berkembang, sehingga harus melibatkan ahli sesuai dengan bidang keahlian yang mereka miliki.
6) Pemberkasaan
   Setelah penyidik berpendapat segala sesuatu pemeriksaan yang diperlukan dianggap cukup, penyidik atasa kekuatan sumpah jabatan segera membuat berita acara. Untuk kelengkapan berita acara, setiap pemeriksaan yang berita acaranya telah dibuat tersendiri dalam kasus pemeriksaan penyidikan, dilampirkan dalam berita acara penyidikan yang dibuat oleh penyidik. Polisi penyidik unit B bidang *Fismondev* unit I/Ekonomi Ditreskrimsus Kepolisian Daerah Bali dalam membuat berita acara penyidikan dan lampiran-lampiran yang bersangkutan dengan kasus penipuan berkedok investasi *online.* Berkas tersebut dijilid menjadi satu berkas. Setelah berkas perkara disempurnakan penjilidaanya maka selanjutnya diserakan kepada Penutut Umum. Penyerahan berkas perkara kepada Penuntut Umum dilakukan dengan dua tahap yaitu tahap pertama, penyidik hanya menyerakan berkas perkara dan tahap kedua, penyidik menyerakan tanggung jawab atas tersangka dan barang bukti hasil penyitaan kepada Penuntut Umum.

Hambatan Kepala Sub Direktorat *Cyber Crime* Dalam Menanggulangi Penipuan Berkedok Investasi *Online* Di Kepolisian Daerah Bali.

Hasil wawancara yang dilakukan peneliti pada tanggal 23 Maret 2018 bersama Bapak Andi Prasetyo SH, mengatakan bahwa Faktor yang menjadi Hambatan Dalam Menanggulangi Penipuan berkedok Investasi *Online* di Kepolisian Daerah Bali adalah:

1) Faktor *Hadware/Software* yang kurang memadai untuk melakukan penyidikan. Hal ini tentunya sangat sulit bagi pihak kepolisian untuk melacak atau mengembangkan lebih lanjut kasus tindak penipuan online karena *softwar*enya kebanyakan ada di luar Polda Bali (Luar Negeri)
2) Anggaran
   Bahwa penipuan online kebanyakan *softwar*enya diluar yuridiksi Polda Bali (Luar Negri) sehingga membutuhkan anggaran yang besar dalam menyelesaikan kasusnya serta ketersediaan dana atau anggaran untuk pelatihan SDM sangat minim sehingga institusi penegak hukum kesulitan untuk mengirimkan mereka mengikuti pelatihan baik didalam maupun diluar negri.
3) Kemampuan Penyidik
   Secara umum Penyidik masih sangat minim dalam penguasaan operasional komputer dan pemahaman terhadap *hacking* komputer serta kemampuan melakukan penyidikan terhadap kasus-kasus kejahatan dunia maya.
4) Alat Bukti
   Persoalan alat bukti yang dihadapi di dalam penyidikan terhadap *cyber crime*

antara lain berkaitan dengan karakteristik kejahatan *cyber crime* itu sendiri. Kesadaran hukum untuk melaporkan kasus ke kepolisian rendah. Hal ini dipicu oleh citra lembaga peradilan itu sendiri yang kurang baik, faktor lain adalah korban tidak ingin kelemahan dalam sistem komputernya diketahui oleh umum, yang berarti akan mempengaruhi kinerja perusahaan dan web masternya.

5) Perangkat hukum yang belum memadai
   Lemahnya peraturan perundang-undangan yang dapa diterapkan terhadap pelaku *cyber crime*, sedangkan penggunaan pasal-pasal yang terdapat didalam KUHP seringkali masih cukup meragukan bagi penyidik. Oleh sebab itu perlu dibuat undang-undang yang khusus mengatur *cyber crime*.
6) Fasilitas komputer forensik
   Untuk membuktikan jejak-jejak para *hacker* dan *cracker* dalam melakukan aksinya terutama yang berhubungan dengan program-program dan data-data komputer, sarana Kepolisian Daerah Bali belum memadai karena belum ada komputer forensik. Fasilitas ini diperlukan untuk mengungkap data-data digital serta merekam dan menyimpan bukti-bukti berupa *soft copy, image*, program dan sebagainya.

IV. SIMPULAN

Berdasarkan penelitian dan pembahasan tentang Peranan Kepala Sub Direktorat *Cyber Crime* Dalam Menanggulangi Penipuan Berkedok Investasi Online Di Kepolisian Daerah Bali dapat disimpulkan bahwa *cyber crime* merupakan perbuatan yang merugikan. Para korban menganggap atau memberi stigma bahwa pelaku *cyber crime* adalah penjahat. Modus operandi *cyber crime* sangat beragam dan terus berkembang sejalan dengan perkembangan teknologi, tetapi jika diperhatikan lebih seksama akan terlihat bahwa banyak di antara kegiatan-kegiatan tersebut memiliki sifat yang sama dengan kejahatan-kejahatan konvensional. Perbedaan umumnya adalah bahwa *cyber crime* melibatkan komputer dalam pelaksanaanya. Kejahatan-kejahatan yang berkaitan dengan kerahasiaan, integrasi dan keberadaan data dan sistem komputer perlu mendapat perhatian khusus, sebab kejahatan-kejahatan ini memiliki karakter yang berbeda dari kejahatan-kejahatan konvensional. Sistem perundang-undangan di Indonesia belum mengatur secara khusus mengenai kejahatan komputer melalui media internet. Beberapa peratura da baik yang terdapat di dalam K upun di luar KUHP untuk sementara dapat diterapkan terhadap beberapa kejahatan, tetapi ada juga kejahatan yang tidak dapat di antisipasi oleh undang-undang yang saat ini berlaku. Adapun Hambatan-hambatan yang ditemukan dalam melakukan penyidikan terhadap *cyber crime* antara lain: Faktor *Hadware/Software* yang kurang memadai untuk melakukan penyidikan, Anggaran, kemampuan penyidik, alat bukti, kesadaran hukum untuk melaporkan kasus ke kepolisian rendah, perangkat hukum yang belum memadai serta fasilitas komputer forensik yang belum memadai sehingga menyulitkan penyidik untuk melakukan penyidikan serta sulit melacak keberadaan pelaku dikarenakan dalam kasus penipuan online bisa siapa saja dan dimana saja orang dapat melakukannya.

Beberapa hal yang dapat dijadikan sebagai saran sehubungan dengan hasil penelitian terhadap *cyber crime* adalah sebagai berikut :

1) Pihak Kepolisian perlu meningkatkan kinerjanya dalam melakukan terhadap kasus penipuan *online* baik secara *preventif, pre-emtif* dan *respresif* yang didukung dengan pemberdayaan sumber daya manusia terutama kepada personil

Kepolisian untuk diberikan pembekalan mengenai ilmu *cyber* yang didukung dengan sarana prasarana yang memadai dibidang teknologi agar dapat secara tegas mengenai kasus *cyber crime* terutama dalam kasus penipuan berkedok investasi *online* yang marak terjadi.

2) Di harapkan kepada pembaca agar dapat lebih mendalami dan memahami secara lebih komprehensif masalah-masalah penipuan dengan cara membandingkan dengan literatur lain, yang pada akhirnya akan terhindar dari segala bentuk penipuan. Karena yang harus diingat, bahwa kejahatan bukan hanya ada niat dari pelaku, tetapi juga karena adanya kesempatan. Berikut, tips bagaimana cara terhindar dari kemungkinan korban *cyber crime*, yaitu:
    a) Perlunya kesadaran dari masyarakat bahwa apa yang ada di dunia maya/internet adalah nyata/fakta
    b) Jangan pernah bertransaksi dengan akun/*website* yang tidak diketahui kredibilitasnya
    c) Jangan pernah mengupload identitas pribadi kedunia maya karena tidak ada yang aman didunia maya walau secanggih apapun proteksinya.

DAFTAR PUSTAKA

Abdul Manap, Nazura. 2001. *Peranan Hukum dalam Penanggulangan Cyber Crime, Kompas Cyber Media* : Jakarta

Arikunto 2010. *Prosedur Penelitian* : *Suatu Pendekatan Praktik.* (Edisi Revisi). Jakarta : Rineka Cipta

Basrom dan Suwandi. 2008. *Memahami Penelitian Kualitatif*. PT. Rineka Cipta: Jakarta

Goodman dan Brenner. 2014 (*Dalam Akbar Kurnia Putra*)

Husein, Umar. 2003. *Metode Riset Komunikasi Organisasi* Jakarta : PT. Gramedia Pustaka Utama.

Jurnal ilmu Hukum Wacana Permata.Hal 80 diakses dijurnal.fhunla.ac.id pada 12 Desember 2016 pukul 10.30 wita

Makarim, Edmon. 2004. *Kompilasi Hukum Telematika*. Raja Grafindo Perkasa :Jakarta

Moelong, Lexy J. 2007. *Metedeologi Penelitian Kualitatif.* Bandung : Remaja Rosdakarya

Nawawi, Hadari. 2001. *Metode Penelitian Sosial*. Yogyakarta : Gajah Mada University Press.

Raharjo, Agus. 2002. *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi.* Citra Aditya Bakti : Bandung
Mengatasi Cyber Crime Jakarta: Grafika Indah

Sugiyono. 2010. *Metode Penelitian Kuantitatif, Kualitatif dan R & D*. Bandung:Alfabeta

Suhariyanto, Budi. 2012. *Tindak Pidana Teknologi Informasi (Cybercrime)* Jakarta : Raja Grafindo Persada.

Suryabrata, Sumadi. 2005. *Metode Penelitian.* Jakarta: Grafika Persada

Wahid, Abdul. dan Mohammad Labib. 2005. *Kejahatan Mayantara (Cyber Crime).* Bandung : Refika Aditama