BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi informasi dan komunikasi yang berkembang secara pesat di dunia menyebabkan perubahan sosial yang drastis sehingga mempermudah masyarakat dalam menerima informasi dan dapat berinteraksi tanpa batasan waktu. Dengan adanya perkembangan ini, secara tidak langsung masyarakat dituntut untuk mengikuti setiap perkembangan yang ada.

Banyak perubahan yang terjadi dalam kehidupan masyarakat akibat adanya pandemi Covid-19 yang berlangsung sekitar setahun ini, salah satunya adalah semakin banyaknya jumlah pengguna internet. Berdasarkan data dari *we are social-Hootsuite,* per Januari 2021 jumlah pengguna internet di Indonesia naik 73,7 persen yakni menembus 202,6 juta pengguna dari 274,9 juta populasi Indonesia. Hal ini menyebabkan terjadinya penambahan 27 juta pengguna dalam setahun terakhir.[1]

Berkembangnya teknologi secara cepat menimbulkan banyak manfaat dan kemudahan dalam segi keamanan, kenyamanan, dan kecepatan dalam melakukan berbagai aktivitas.[2] Pemanfaatan teknologi informasi dan komunikasi yang tidak terbatas, selain memberikan dampak positif juga

[1]Simon Kemp, *Digital 2021: The Latest Insights Into The 'State Of Digital'*, https://wearesocial.com/uk/blog/2021/01/digital-2021-the-latest-insights-into-the-state-of-digital/, diakses pada tanggal 30 Januari 2021, pukul 05:42 WIB.

[2] Achmad Sadiki, 2005, *Kejahatan Mayantara (Cyber Crime)*, Bandung, Refika Aditama, hlm. 13.

memberikan dampak negatif yakni munculnya modus kejahatan baru yang biasa dikenal dengan *cybercrime*.[3] Karakteristik *Cybercrime* bersifat umum dengan ciri khusus yaitu orang yang melakukan kejahatan tersebut mampu menguasai penggunaan internet secara keseluruhan.[4]

Salah satu jenis kejahatan siber yang sering terjadi pada media online adalah penipuan *online*. Penipuan *online* merupakan kejahatan yang dilakukan seseorang melalui internet untuk kepentingan bisnis sehingga tidak perlu bergantung pada perusahaan bisnis konvensional.[5] Prinsip penipuan *online* sama seperti penipuan konvensional, perbedaannya terletak pada alat yang digunakan yakni menggunakan perangkat komputer, jaringan internet, serta perangkat telekomunikasi. Penipuan *online* tidak hanya terjadi di dalam negeri tetapi juga di luar negeri. Hal ini mengakibatkan kerugian bagi masyarakat maupun negara.[6]

Menurut peneliti keamanan siber, Pratama Persadha dari Communication Information System Security Research Center (CISSReC), mengatakan bahwa peningkatan kasus penipuan online sebanding dengan pencurian data pribadi yang menjadi bahan utama kejahatan siber. Terdapat

---

[3] Widodo, 2011, *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law); Telaah Teoritik dan Bedah Kasus*, Yogyakarta, Aswaja Presindo, hlm. 12.

[4] Asril Sitompul, 2001, *Hukum Internet: Pengenalan Mengenai Masalah Hukum di Cyberspace.* Bandung, Citra Aditya Bakti, hlm. 8.

[5] Desy Setyowati, *Marak Penipuan Online saat Konsumen Hijrah ke Digital di Masa Pandemi*, https://katadata.co.id/desysetyowati/digital/600aa5de3a818/marak-penipuan-online-saat-konsumen-hijrah-ke-digital-di-masa-pandemi, diakses pada tanggal 28 Januari 2021, pukul 13.30 WIB.

[6] Josua Sitompul, 2012, *Cyberspace Cybercrime Cyberlaw Tinjauan Aspek Hukum Pidana*, Jakarta, Tatanusa, hlm. 31.

banyak modus penipuan online di Indonesia, antara lain seperti modus menawarkan produk elektronik dengan harga murah, modus investasi bodong, modus mencuri akun mitra pengemudi Gojek atau Grab, modus penipuan menggunakan fitur pengalihan panggilan (*call forward*), serta modus menipu korban belanja online di media sosial. [7]

Dilihat dari segi hukum, penipuan online dapat dianggap sama sebagai delik konvensional yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP). Tetapi penipuan online diatur secara khusus dalam undang-undang nomor 19 tahun 2016 tentang perubahan atas undang-undang 11 tahun 2008 tentang Informasi dan Transaksi elektronik. UU ITE tidak secara rinci menyatakan adanya tindak pidana penipuan, tetapi secara implisit terdapat unsur yang hampir sama dengan tindak pidana penipuan yang diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP).[8]

Dikutip dari artikel Tirto.id, UU ITE merupakan hasil kerja kolektif dari berbagai kementerian seperti kementerian perhubungan, kementerian perindustrian, dan kementerian perdagangan. Menurut Anton Muhajir dari SAFEnet, setidaknya ada sekitar 3.100 kasus terkait pasal-pasal dalam UU

[7] Maskun, 2013, *Kejahatan Siber (Cyber Crime) Suatu Pengantar*, Jakarta, Kencana Prenada Media Group, hlm. 129.

[8] Alexander Haryanto, *Apa Itu UU ITE & Isi Aturan Nomor 11 Tahun 2008 Pasal 27 Sampai 31?*, https://tirto.id/apa-itu-uu-ite-isi-aturan-nomor-11-tahun-2008-pasal-27-sampai-31-gaj7, diakses pada tanggal 25 Februari 2021, pukul 21:56 WIB.

ITE sepanjang 2019.[9] Dengan adanya undang-undang tersebut dapat ditangguhkan dan wajib di himbau oleh seluruh Warga Negara Indonesia, saat ini Indonesia merupakan salah satu negara yang telah menggunakan serta memanfaatkan teknologi informasi secara luas dan efisien. Undang-undang tentang Informasi dan Transaksi Elektronik ini sangatlah memberikan banyak manfaat, seperti menjamin kepastian hukum bagi masyarakat yang melakukan transaksi elektronik, mencegah terjadinya kejahatan berbasis teknologi informasi, mendorong pertumbuhan laju ekonomi, dan melindungi masyarakat pengguna jasa yang memanfaatkan teknologi informasi.

Penegakan hukum di Indonesia pada saat ini mengalami kesulitan dalam menghadapi merebaknya kejahatan siber *(cybercrime)*. Hal ini dilatarbelakangi dengan masih sedikitnya aparat penegak hukum yang memahami seluk beluk teknologi informasi (internet), terbatasnya sarana dan prasarana, serta kurangnya kesadaran hukum masyarakat dalam upaya penanggulangan tindak pidana teknologi informasi, biaya peralatan yang mahal. Hal ini disebabkan oleh masih banyaknya institusi-institusi penegak hukum di daerah yang belum didukung dengan jaringan internet yang memadai.

[9] Pipit Ika Ramadhani, *Bareskrim Catat Ada 1.617 Kasus Penipuan Online pada 2019, Paling Banyak di Instagram*, https://www.liputan6.com/bisnis/read/4369038/bareskrim-catat-ada-1617-kasus-penipuan-online-pada-2019-paling-banyak-di-instagram, diakses pada tanggal 21 Februari 2021, pukul 08:03 WIB.

POLRI memiliki unit khusus melakukan penanganan *cybercrime* sejak 2002, unit ini bertugas untuk melakukan penegakan hukum terhadap kejahatan siber. Pada tanggal 7 februari 2017, semakin banyaknya pengguna internet dan teknologi informasi maka POLRI memperkuat dirinya dengan membentuk Direktorat Tindak Pidana Siber Bareskrim guna melakukan penegakan hukum terhadap kejahatan siber dalam sekala nasional maupun transnasional.

Penegakan hukum diberikan kepada kepolisian yang diberi kewenangan mengemban fungsi reserse yang biasa disebut penyidik. Berdasarkan kitab undang-undang Hukum Acara Pidana pasal 6 ayat (1) berbunyi "Penyidik adalah pejabat polisi Negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang-undang untuk melakukan penyidikan." Penyidikan dilakukan sehingga penyelesaian kasus ini menjadi bagian penegakan hukum, polisi dituntut profesional dalam pemberantasan tindak pidana apapun termasuk *cybercrime* demi menciptakan keamanan bagi masyarakat.

Sepanjang 2019, Direktorat Tindak Pidana Siber Bareskrim mencatat terdapat 1.617 kasus teratas yakni penipuan online. Rinciannya sebanyak 534 kasus di Instagram, 413 di whatsapp, dan sisanya 304 kasus terjadi di Facebook. Pihak kepolisian mencatat laporan penipuan online di tahun 2019 tergolong ekstrim. Menurut Polda Metro Jaya, tahun lalu kasus penipuan online paling banyak diadukan dengan 2.300 laporan. Modus rekayasa sosial *(social engineering)* digunakan untuk berbagai bentuk

penipuan online, biasanya digunakan untuk melakukan pengurasan saldo rekening, kartu kredit, dan maupun saldo dompet digital.[10]

Dikutip dari artikel tirto.id, Selama tanggal 23 Februari sampai 19 Maret 2021, polisi virtual Direktorat Tindak Pidana Siber Polri telah memberi peringatan terhadap 189 akun yang berpotensi mengganggu ketertiban dunia maya. Hal ini dijelaskan lebih lanjut oleh Kepala Bagian Penerangan Umum Divhumas Polri, Kombes Pol Ahmad Ramadhan, bahwa terdapat 105 konten yang telah dinyatakan lolos verifikasi dengan memenuhi unsur ujaran kebencian, sedangkan 52 konten tidak lolos verifikasi, dan 32 konten sedang dalam proses verifikasi. Kepolisian siber juga meciptakan program baru berupa *"Badge Award"*, penghargaan ini diberikan kepada masyarakat yang berhasil melaporkan dan memberikan informasi berupa tindak pidana di media sosial yang telah terverifikasi.[11]

B. Rumusan Masalah

1. Apa faktor-faktor yang menyebabkan terjadinya tindak pidana penipuan online?
2. Bagaimana penegakan hukum terhadap tindak pidana penipuan online oleh Direktorat Tindak Pidana Siber Bareskrim POLRI?

---

[10] Adi Briantika, *Polisi Virtual Temukan 189 Konten Gangguan Siber per Februari-Maret,* https://tirto.id/polisi-virtual-temukan-189-konten-gangguan-siber-per-februari-maret-gbqA, diakses pada tanggal 25 Januari 2021, pukul 22:10 WIB.

[11] Wirjono Prodjodikoro, 2003, *Tindak-Tindak Pidana Tertentu di Indonesia,* Bandung, Refika Aditama, hlm. 1.

C. Tujuan Penelitian

1. Untuk mengetahui dan mengkaji faktor-faktor yang menyebabkan tindak pidana penipuan online oleh Direktorat Tindak Pidana Siber Bareskrim POLRI.
2. Untuk mengetahui penegakan hukum terhadap tindak pidana penipuan online oleh Direktorat Tindak Pidana Siber Bareskrim POLRI.

D. Manfaat Penelitian

1. Manfaat Teoritis

   a. Hasil penelitian ini diharapkan dapat digunakan sebagai pengembangan ilmu hukum khususnya Hukum Pidana yang berkenaan dengan penegakan hukum terhadap tindak pidana penipuan online.

   b. Hasil penelitian ini diharapkan dapat melatih pengembangan pola pikir yang sistematis dan digunakan untuk mengukur kemampuan penulis dalam menerapkan ilmu yang telah didapatkan.

E. Tinjauan Pustaka

1. Pengertian Tindak Pidana

Menurut Wirjono Prodjodikoro, Tindak pidana merupakan pelanggaran norma-norma dalam tiga bidang hukum, yaitu yang pertama Hukum Perdata, kedua Hukum Ketatanegaraan, dan terakhir Hukum Pidana, dapat dikatakan suatu tindak pidana jika memiliki sifat

melanggar hukum.[12] Tindak Pidana dikenal dengan istilah Belanda yakni "*Strafbaar Feit*" atau "*Delik*". Menurut K. Wantjik Saleh, terdapat enam istilah untuk menerjemahkan istilah "*strafbaar feit"* atau*"* delik*"* ini, yakni sebagai berikut:[13]

a. Perbuatan yang boleh dihukum
b. Peristiwa pidana
c. Pelanggaran pidana
d. Perbuatan pidana
e. Tindak pidana

2. Tindak Pidana Siber (*Cyber Crime*)

a. Definisi *Cyber Crime*

Pada mulanya, *cybercrime* didefinisikan sebagai kejahatan komputer *(Computer Crime)*. *The British Law Commission*, mengartikan kejahatan komputer sebagai bentuk kecurangan yang dilakukan dengan menggunakan alat komputer guna memperoleh uang, barang, dan keuntungan lain sehingga menimbulkan kerugian pada pihak lain. Mandell membagi *"computer crime"* atas dua kegiatan, yaitu:

1) Perbuatan penipuan, pencurian, penyembunyian dengan menggunakan komputer sebagai alat untuk memperoleh keuntungan keuangan, bisnis, dan juga kekayaan;

[12] Wantjik K Saleh. 1996, *Tindak Pidana Korupsi dan Suap*, Jakarta, Paramestika, hlm. 15.
[13] Budi Suhariyanto, 2013, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*, Jakarta, Rajawali Pers., hlm 10.

2) Ancaman terhadap komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan.[14] Sistem teknologi informasi yang berbentuk internet dapat berpengaruh terhadap pola pikir para ahli hukum terhadap definisi kejahatan computer. Awal mulanya para ahli hukum lebih mengutamakan pada alat/perangkat keras yaitu komputer. Namun seiring perkembangan tersebut maka fokus dari identifikasi terhadap definisi *cybercrime* lebih diperluas lagi yaitu seluas aktivitas yang dapat dilakukan di dunia cyber/maya melalui sistem informasi yang digunakan. Jadi tidak sekedar pada komponen *hardware*-nya saja kejahatan itu dimaknai sebagai *cybercrime*, tetapi sudah dapat diperluas dalam lingkup dunia yang dijelajah oleh sistem teknologi informasi yang bersangkutan. sehingga lebih tepat jika pemaknaan dari *cybercrime* adalah kejahatan teknologi informasi, juga sebagai kejahatan mayantara. *Cybercrime* adalah kejahatan yang dilakukan di dunia maya dengan menggunakan computer dan jaringan teknologi yang disediakan oleh Infrastruktur Informasi dan Komunikasi.[15] Pada dasarnya *cybercrime* meliputi semua tindak pidana yang berkenaan dengan sistem informasi itu sendiri, serta sistem

[14] Ibid. hlm 11
[15] Mochammad Fahlevi, Mohamad Saparudin, Sari Maemunah, Dasih Irma, and Muhamad Ekhsan. "Cybercrime Business Digital in Indonesia", *Jurnal ICENIS*, Vol 1 No 125 (2019), hlm. 2.

informasi yang merupakan sarana untuk penyampaian/pertukaran informasi kepada pihak lainnya.

b. Karakteristik Cyber Crime

Kejahatan dibidang teknologi informasi dapat digolongkan sebagai *White Collar Crime* karena pelaku *cybercrime* dapat menguasai penggunaan internet beserta aplikasinya atau ahli di bidangnya. Kejahatan tersebut kerap kali dilakukan secara transnasional atau melintasi batas negara sehingga dua kriteria dalam kejahatan siber ini, yaitu *White Collar Crime* dan *Transnational Crime.*[16]

Berdasarkan literatur serta praktiknya, *cybercrime* memiliki beberapa karakteristik, yaitu:[17]

1) Perbuatan illegal, yang terjadi dalam ruang siber/*cyber space*, sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.
2) Perbuatan dilakukan dengan alat apapun yang terhubung melalui internet.
3) Perbuatan menimbulkan kerugian yang cenderung lebih besar dibandingkan dengan kejahatan konvensional berupa kerugian

[16] Ari Dermawan & Akmal, "Urgensi Perlindungan Hukum Bagi Korban Tindak Pidana Kejahatan Teknologi Informasi", *Journal of Science and Social Research,* Vol 2 No 2 (2019). hlm. 39-46

[17] Adami Chazawi, 2011, *Pelajaran Hukum Pidana (Stelsel Tindak Pidana, Teori-Teori Pemidanaan & Batas Berlakunya Hukum Pidana*, Jakarta, Raja Grafindo Persada, hlm. 79.

materiil maupun immateriil (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi).

4) Pelakunya dapat menguasai penggunaan internet beserta aplikasinya.
5) Perbuatan sering dilakukan secara transnasional/melintasi batas negara.

3. Tindak Pidana Penipuan *Online*

Tindak Pidana yang dilakukan dalam lingkup dunia maya biasa disebut dengan *cybercrime.* salah satu jenis kejahatannya adalah penipuan *online.* Tindak pidana penipuan *online* adalah salah satu jenis kejahatan yang memanfaatkan perkembangan ilmu pengetahuan dan teknologi informasi, dengan modus menyebarkan informasi tidak benar melalui internet yang bertujuan menipu calon korbannya untuk mendapatkan keuntungan. Kasus penipuan *online* telah diatur di dalam UU ITE. [18]

4. Upaya Penanggulangan Tindak Pidana Penipuan Online oleh Direktorat Tindak Pidana Siber Bareskrim Polri

Dalam menanggulangi terjadinya terjadinya kasus *cybercrime* yakni penipuan online, pihak kepolisian telah melakukan berbagai upaya penanggulangan, yakni :

[18] Ana Maria F Pasaribu, Syahrin, Alvi, Hasibuan, Syafruddin, "Kejahatan Siber Sebagai Dampak Negatif Dari Perkembangan Teknologi dan Internet Di Indonesia Berdasarkan Undang-Undang No. 19 Tahun 2016 Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Persfektif Hukum Pidana", *Jurnal Hukum,* Vol 1 No 1 (2017), hlm. 13-14.

a. Merespon dan menerima setiap pengaduan dari masyarakat atas dugaan terjadinya tindak pidana Siber serta mendata setiap penanganan kasus terhadap pengaduan serta laporan dari masyarakat tentang tindak pidana Siber*;*
b. Melakukan penyelidikan secara online (penyelidikan melalui internet) terhadap kejahatan-kejahatan yang menggunakan jejaring sosial facebook, email dan penjualan secara online;
c. Melakukan kerjasama dengan Kementrian Komunikasi dan Informatika (Kominfo);
d. Melakukan kerjasama dengan bidang perbankan khususnya Bank Indonesia, untuk menghindari rekening dengan identitas palsu yang nantinya digunakan oleh para pelaku kejahatan Informasi Transaksi Elektronik (ITE);
e. Menginformasikan kepada masyarakat untuk lebih waspada dalam menggunakan internet;
f. Meningkatkan pemahaman serta keahlian Polri di bidang *cybercrime* dengan mengirimkan anggotanya untuk mengikuti berbagai macam pelatihan di berbagai negara maju.

5. Penegakan Hukum

Penegakan hukum tidak bisa dipisahkan dari badan peradilan (penegak hukum) dan hukumnya sendiri. Ketiganya menjadi pilar yang saling menopang dan tidak bisa dipisahkan. Hukum itu berguna bila ditegakkan oleh lembaga peradilan. Sebaliknya, penegakan hukum tidak

akan bisa berjalan jika tidak ada hukum sebagai landasan bagi lembaga peradilan dalam menegakkan hukum. Tidak ada yang lebih utama dari ketiga hal itu. Maka dari itu, ketiganya harus bekerja secara sinergis serta berjalan secara seimbang.

F. Metode Penelitian

1. Jenis Penelitian

Penelitian ini merupakan penelitian yuridis empiris yaitu penelitian hukum mengenai pemberlakuan atau implementasi ketentuan hukum normatif secara langsung pada setiap peristiwa hukum tertentu yang terjadi dalam masyarakat. Penelitian dilakukan dengan wawancara langsung terhadap pihak yang dianggap mengetahui dan ada kaitannya dengan permasalahan yang akan dibahas dan diperoleh di lokasi penelitian tentang faktor-faktor serta penegakan hukum yang berkaitan dengan penegakan hukum terhadap tindak pidana penipuan online.

2. Sumber Data

Sumber data dalam penelitian ini terdiri atas data primer dan data sekunder :

a. Data Primer, yaitu sumber data berdasarkan hasil penelitian lapangan melalui wawancara terhadap narasumber yakni penyidik Direktorat Tindak Pidana Siber Bareskrim POLRI dan memberikan angket

terhadap para responden yakni korban kasus laporan polisi di Jakarta Selatan.

b. Data sekunder, yaitu data dan informasi yang penulis peroleh secara tidak langsung, melalui data dan dokumen yang telah tersedia pada instansi atau tempat penelitian penulis. Adapun sumber data yang penulis peroleh berasal dari peraturan perundang-undangan, pendapat pakar hukum, serta laporan yang ada. Data sekunder terdiri dari tiga bahan pustaka yang terdiri dari:

1) Bahan Hukum Primer

Bahan hukum primer adalah bahan hukum yang mengikat, terdiri atas peraturan perundang-undangan yang berlaku atau ketentuan-ketentuan yang berlaku. Sehubungan dengan itu, maka bahan hukum primer yang digunakan yaitu:

a) Undang Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)
b) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE)
c) Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana

2) Bahan Hukum Sekunder

Bahan hukum sekunder adalah bahan hukum yang dapat memberikan penjelasan mengenai bahan hukum primer, yang meliputi pendapat hukum, buku literatur, jurnal ilmiah, hasil penelitian, surat kabar, berita intenet dan lain sebagainya yang berhubungan dengan judul penulisan hukum ini.

3) Bahan Hukum Tersier

Bahan hukum tersier merupakan bahan hukum yang mendukung bahan hukum primer dan bahan hukum sekunder yang berupa kamus, ensiklopedia, indeks komulatif, dan terminologi hukum.

3. Narasumber dan Responden

a. Narasumber merupakan seseorang yang mengetahui secara jelas dan dapat memberikan pendapat terhadap informasi yang diberikan.

   Narasumber dalam penelitian ini adalah penyidik Direktorat Tindak Pidana Siber Bareskrim POLRI : IPTU Stephanie K Brennadiva, S.Si, S.Pd, MISDF.

b. Responden merupakan penjawab atas pertanyaan yang diajukan untuk kepentingan penelitian.

   Responden dalam penelitian ini adalah para korban kasus laporan polisi di Jakarta Selatan. Korban terdiri dari 10 orang.

4. Teknik Pengumpulan Data

a. Studi Pustaka

Dalam penelitian ini pengumpulan data sekunder dilakukan dengan studi kepustakaan, yakni dengan membaca dan melakukan penelurusan sumber melalui jurnal, buku, dan peraturan perundang-undangan sebagai bahan penelitian yang berkaitan dengan kejahatan dunia maya.

b. Studi Lapangan

Dalam penelitian ini pengumpulan data primer dilakukan dengan studi lapangan yang dilakukan dengan cara :

1) Wawancara

Wawancara dengan melakukan pengumpulan data dengan cara tanya jawab langsung antara peneliti dengan narasumber atau respoden yang dapat memberikan informasi tentang obyek yang diteliti baik menggunakan daftar pertanyaan maupun tanya jawab secara bebas, penulis melakukan wawancara kepada penyidik Direktorat Tindak Pidana Siber Bareskrim POLRI : IPTU Stephanie K Brennadiva, S.Si, S.Pd, MISDF.

2) Angket

Angket merupakan pertanyaan tertulis yang diedarkan kepada responden untuk mengumpulkan informasi. Angket yang digunakan penulis berupa *google form* untuk mengetahui permasalahan faktor yang menjadi kecendrungan meningkatnya

penipuan online, ditujukan kepada responden korban tindak pidana penipuan online yang terdiri dari 10 orang.

5. Lokasi Penelitian

Lokasi yang akan digunakan untuk penelitian dilakukan di Direktorat Tindak Pidana Siber Bareskrim POLRI.

6. Metode Analisis Data

Pada penelitian ini, Analisis data mengunakan analisis kualitatif yang bersifat deskriptif. Analisis kualitatif yaitu teknik yang mengambarkan keadaan yang sebenarnya secara menyeluruh berdasarkan data yang telah dikumpulkan. Kemudian data tersebut dianalisis dengan deskriptif kedalam pembahasan penelitian dalam bentuk kalimat yang memberikan gambaran apakah berjalan sesuai mengenai kejahatan penipuan online.

G. Sistematika penulisan skripsi

Skripsi ini terbagi dalam 5 (lima) bab, dimana masing-masing bab memiliki keterkaitan antara satu bab dengan lainnya. Sistematika penulisan ini bertujuan agar penulisan skripsi ini terarah dan sistematis. Adapun sistematika dalam penelitian ini adalah sebagai berikut:

BAB I Bab ini terdiri dari enam sub bab yang diantaranya adalah : Latar Belakang Masalah, Rumusan Masalah, Tujuan Penelitian, Manfaat Penelitian, Tinjauan Pustaka, Metode

Penelitian dan Sistematika Penulisan Skripsi. Isi Bab I ini akan digunakan sebagai pedoman bagi Tinjauan Pustaka pada Bab II dan Bab III dan akan menjadi bahan analisis untuk menganalisa hasil penelitian pada Bab IV.

BAB II Berisi tentang Tinjauan Umum tentang Tindak Pidana Penipuan *Online* yang membahas mengenai Tindak Pidana, Tindak Pidana Siber *(Cybercrimes),* dan juga Tindak Pidana Siber (Penipuan *online)*.

BAB III Pada bab ini membahas tentang Penegakan Hukum terhadap Tindak Pidana Penipuan *Online*, yang akan diuraikan mengenai Penegakan Hukum, Peran Direktorat Tindak Pidana Siber Bareskrim POLRI serta Hambatan dalam Penegakan Hukum Tindak Pidana Penipuan Online.

BAB IV Berisi mengenai analisis hasil wawancara yang telah dilakukan oleh penulis dalam faktor-faktor yang menyebabkan terjadinya tindak pidana penipuan *online* dan penegakan hukum terhadap tindak pidana penipuan *online* oleh Direktorat Tindak Pidana Siber Bareskrim POLRI. Nantinya akan ditarik kesimpulan terhadap hasil penelitian yang akan dijelaskan pada bab V.

BAB V Pada bab ini akan membahas penutup yang berisikan kesimpulan dan saran dari hasil penelitian yang telah dilakukan oleh penulis.