

UNIVERSITAS KATOLIK PARAHYANGAN

FAKULTAS HUKUM

Terakreditasi Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi

Nomor : 429/SK/BAN-PT/Akred/S/XI/2014

**KEJAHATAN PEMERASAN MENGGUNAKAN VIRUS *RANSOMWARE*
DIKAITKAN DENGAN KEJAHATAN ITE**

Oleh

Kevin Anthony

NPM : 2017200001

Dosen Pembimbing :

1. R. Ismadi Santoso Bekti, S.H., M.H.



Penulisan Hukum

Disusun Sebagai Salah Satu Kelengkapan

Untuk Menyelesaikan Program Pendidikan Sarjana

Program Studi Ilmu Hukum

2024

Penulisan Hukum dengan judul
KEKJAHATAN PEMERASAN DENGAN MENGGUNAKANA VIRUS *RANSOMWARE*
DIKAITKAN DENGAN KEJAHATAN ITE

yang ditulis oleh:

Nama: Kevin Anthony

NPM: 2017200001

Pada tanggal: 09/08//2024

Telah disidangkan pada

Ujian Penulisan Hukum Program Studi Hukum Program Sarjana

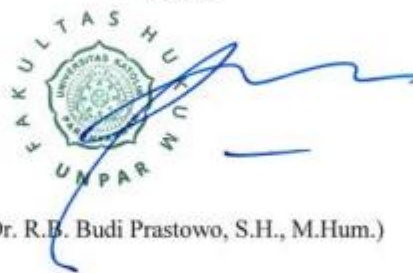
Fakultas Hukum Universitas Katolik Parahyangan

Pembimbing



(R. Ismadi Santoso Bektu, S.H., M.H.)

Dekan,



(Dr. R.B. Budi Prastowo, S.H., M.Hum.)



PERNYATAAN INTEGRITAS AKADEMIK

Dalam rangka mewujudkan nilai-nilai ideal dan standar mutu akademik yang setinggi-tingginya, maka Saya, Mahasiswa Fakultas Hukum Universitas Katolik Parahyangan yang beranda tangan di bawah ini :

Nama : Kevin Anthony

NPM : 2017200001

Dengan ini menyatakan dengan penuh kejujuran dan dengan kesungguhan hati dan pikiran, bahwa karya ilmiah / karya penulisan hukum yang berjudul:

“KEJAHATAN PEMERASAN MENGGUNAKAN VIRUS RANSOMWARE DIKAITKAN DENGAN KEJAHATAN ITE”

Adalah sungguh-sungguh merupakan karya ilmiah /Karya Penulisan Hukum yang telah saya susun dan selesaikan atas dasar upaya, kemampuan dan pengetahuan akademik Saya pribadi, dan sekurang-kurangnya tidak dibuat melalui dan atau mengandung hasil dari tindakan-tindakan yang:

- Secara tidak jujur dan secara langsung atau tidak langsung melanggar hak-hak atas kekayaan intelektual orang lain, dan atau
- Dari segi akademik dapat dianggap tidak jujur dan melanggar nilai-nilai integritas akademik dan itikad baik;

Seandainya di kemudian hari ternyata bahwa Saya telah menyalahi dan atau melanggar pernyataan Saya di atas, maka Saya sanggup untuk menerima akibat-akibat dan atau sanksi-sanksi sesuai dengan peraturan yang berlaku di lingkungan Universitas Katolik Parahyangan dan atau peraturan perundang-undangan yang berlaku.

Pernyataan ini Saya buat dengan penuh kesadaran dan kesukarelaan, tanpa paksaan dalam bentuk apapun juga.

Bandung, 30 Juli 2024

Mahasiswa penyusun Karya Ilmiah/ Karya Penulisan Hukum

()
993ALX297449361

Kevin Anthony

NPM

“Kejahatan Pemerasan Menggunakan Virus *Ransomware* Dikaitkan Dengan kejahatan ITE”

Oleh :

Kevin Anthony (2017200001)

Pembimbing :

R. Ismadi Santoso Bakti, S.H., M.H.

ABSTRAK

Tindak kejahatan sudah sejak lama ada dan tidak terlepas dari kehidupan setiap manusia dalam melakukan interaksi dengan orang lain. Adanya kehidupan masyarakat yang semakin berkembang dan semakin modern, telah menciptakan sebuah teknologi yang dikenal dengan sebutan internet dan komputer. Dalam perkembangan zaman, teknologi dan masyarakat yang telah berkembang menjadi semakin modern telah menciptakan sebuah tindak pidana siber yang merupakan sebuah kejahatan baru yang melibatkan sebuah komputer sebagai alat untuk melakukan tindak kejahatan maupun sistem komputer tersebut yang menjadi target dari tindak kejahatan. Semakin berkembangnya tindak pidana siber dalam masyarakat saat ini, menciptakan jenis – jenis kejahatan siber yang beragam seperti *ransomware*. *Ransomware* yang merupakan sebuah program yang berfungsi untuk melakukan penguncian data dengan tujuan untuk meminta tebusan kepada korban agar dapat melakukan akses terhadap data yang terdapat dalam sistem komputer yang telah dikunci tersebut. Kejahatan *ransomware* ini melibatkan sistem komputer dan juga tindak kejahatan pemerasan yang dilakukan oleh pelaku kejahatan. Dengan adanya sebuah kejahatan *ransomware* penulis hendak meninjau bagaimana pertanggung jawaban pelaku kejahatan *ransomware* di Indonesia dan apa saja tindakan penanggulangan yang dapat dilakukan oleh pemerintah dan masyarakat untuk menindak maupun mencegah terjadinya kejahatan *ransomware* yang sudah terdapat dalam masyarakat saat ini.

(Kata Kunci : *Ransomware*, kejahatan siber, pertanggungjawaban pidana, pemerasan, virus, ITE)

“Extortion Crimes Using Ransomware Viruses Are Associated with ITE Crimes”

By:

Kevin Anthony (2017200001)

Conselor :

R. Ismadi Santoso Bekti, S.H., M.H.

ABSTRACT

Crime has long existed and is inseparable from the life of every human being in every interacting with others. The existence of a society that is increasingly developing and increasingly modern, has created a technology known as the internet and computers. In the development of the times, technology and society that has developed into an increasingly modern society has created a cybercrime which is a new crime involving a computer as a tool to commit a crime and the computer system which is the target of the crime. The development of cyber crime in today's society has created various types of cyber crime, such as ransomware. Ransomware is a program with fuction to lock data in computer system and then the criminals will ask for ransom for gain access to the data contained in the locked computer system. This ransomware crime involves computer systems and also extortion crimes committed by criminals. With the existence of a ransomware crime, the author wants to review the responsibility of the perpetrators of ransomware crimes in Indonesia and what countermeasures can be taken by the government and society to crack down and prevent the occurrence of ransomware crimes that are already in today society.

(Keywords: Ransomware, cybercrime, criminal liability, extortion, virus, ITE)

KATA PENGANTAR

Puji Syukur penulis panjatkan kepada Tuhan yang Maha Esa atas berkat, rahmat, dan anugerah sehingga penulis dapat menyelesaikan tugas akhir berjudul “KEJAHATAN PEMERASAN MENGGUNAKAN VIRUS *RANSOMWARE* DIKAITKAN DENGAN KEJAHATAN ITE”. Skripsi ini dibuat untuk memenuhi salah satu syarat untuk memperoleh Sarjana Hukum pada Fakultas Hukum Program Studi Ilmu Hukum Universitas Katolik Parahyangan. Terlepas dari itu penulis berharap bahwa tulisan ini dapat bermanfaat bagi pembaca.

Dalam proses penyusunan skripsi ini tidak terlepas dari bantuan dan dukungan dari berbagai pihak. Pada kesempatan ini, penulis ingin menyampaikan kepada seluruh pihak atas dukungan dan bantuan serta bimbingan yang telah diberikan kepada penulis hingga dapat menyelesaikan penyusunan skripsi ini. Dengan segala kerendahan hati, penulis ingin mengucapkan terima kasih khususnya kepada:

1. R. Ismadi Santoso Bekti, S.H., M.H. selaku dosen pembimbing penulis yang telah sabar memberikan dukungan, saran, waktu, perhatian, dan selalu bersedia membantu penulis menyelesaikan laporan skripsi ini.
2. Dr. R.B. Budi Prastowo, S.H., M.Hum. selaku dosen penguji yang telah memberikan masukan, saran, kritik, dan arahan untuk proses penyusunan laporan skripsi ini.
3. Keluarga penulis yang selalu memberikan dukungan, doa, motivasi dan siap membantu penulis dalam segala hal untuk menyelesaikan penyusunan skripsi ini.
4. Seluruh dosen UNPAR terutama dosen – dosen jurusan hukum yang telah memberikan bantuan serta ilmu selama penulis menempuh pendidikan.
5. William Laurent, Coach Matthew Yoan Rijota, Krisanti Franssisca Ribenty Setiawan S.Ds., Tahlita Priscillia Eliezer, S.Pd, Darren Christopher Yo, Albert Huang selaku sahabat yang telah memberikan bantuan dan dukungan kepada penulis.
6. Seluruh teman penulis di STARWOTS yang telah memberikan dukungan dan doa kepada penulis.
7. Selurus mahasiswa jurusan Ilmu Hukum UNPAR atas kebersamaannya menempuh pendidikan.
8. Seluruh pihak yang terkait dengan penulis dalam pembuatan laporan skripsi.

Penulis menyadari laporan skripsi ini masih jauh dari kata sempurna oleh sebab itu penulis menerima saran dan kritik yang dapat membangun. Semoga penulisan hukum ini dapat bermanfaat bagi pembaca.

DAFTAR ISI

BAB I PENDAHULUAN.....	8
1.1 Latar Belakang Masalah.....	8
1.2 Rumusan Masalah	12
1.3 Tujuan Penelitian	12
1.4 Metode Penelitian	12
1.5 Sistematika Penulisan	13
BAB II KAJIAN TENTANG PENGGUNAAN VIRUS UNTUK PEMERASAN	15
2.1 Virus	15
2.2 Pemerasan	17
2.3 Metode Penyebaran	19
2.4 Ransomware	20
2.5 Contoh kasus	29
BAB III Kajian Tentang Kejahatan yang Berhubungan Dengan Informasi dan Transaksi Elektronik	32
3.1. Kejahatan Informasi dan Transaksi Elektronik	36
3.2. Internet	38
3.3. Cybercrime	40
3.4. Malware	46
3.5. Extra Yurisdiksi	48
BAB IV ANALISIS PENGGUNAAN VIRUS DALAM KEJAHATAN PEMERASAN	51
4.1 Pertanggungjawaban Pidana Pelaku Kejahatan Pemerasan dengan Menggunakan Virus	51

4.2 Upaya Perlindungan Korban Serangan Ransomware	62
BAB V PENUTUP	68
5.1 Kesimpulan	68
5.2 Saran	70
DAFTAR PUSTAKA	71

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Pasal 1 ayat 3 UUD Negara Republik Indonesia Tahun 1945 menyatakan bahwa Negara Indonesia adalah Negara Hukum yang berarti semua hal yang dilakukan harus dalam penyelenggaraan maupun kegiatan masyarakat sesuai dengan aturan hukum yang berlaku. Dalam kehidupan sehari-hari masyarakat Indonesia menggunakan sebuah teknologi yang dikenal dengan Internet yang menciptakan sebuah hubungan tanpa batasan jarak maupun batas negara.¹ Dengan adanya internet yang menjadikan hubungan antara manusia semakin mudah tanpa perlu memikirkan adanya batasan jarak dan waktu untuk melakukan interaksi dengan satu dengan yang lain membuat pengguna dari internet semakin populer di kalangan masyarakat, dengan demikian adanya internet ini semakin meningkat dari tahun ke tahunnya. Menurut data yang dimiliki oleh pemerintah Indonesia pada tahun 2021 adalah 202,6 juta pengguna dan pada tahun 2022 meningkat menjadi 215 juta pengguna lalu tahun 2023 lalu bertambah menjadi 221 juta pengguna internet.² Peningkatan jumlah pengguna internet di Indonesia sendiri tidak serta merta karena adanya perkembangan teknologi dan telekomunikasi, hal ini juga didukung oleh pemerintah Indonesia yang memajukan perkembangan infrastruktur yang membuat kemudahan dalam pengembangan dan pembangunan jaringan internet dan telepon seluler demi meningkatkan konektivitas di seluruh negeri terutama daerah - daerah pedesaan yang sebelumnya sulit untuk dijangkau.

Dengan perkembangan informasi dan telekomunikasi yang semakin canggih, membuat perkembangan teknologi lain juga semakin berkembang dengan pesat seperti perkembangan telepon yang pada awalnya hanya berupa telepon yang tidak dapat dibawa kemana - kemana hingga di zaman sekarang berkembang menjadi telepon yang lebih kecil dan mudah di bawa

¹ Nudirman Munir. *Pengantar Hukum Siber Indonesia*. Rajawali Pers: Depok, 2017, hal 5.

² Asosiasi Penyelenggara Jasa Internet Indonesia, *APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang*, [https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20\(APJII\)%20mengumumkan%20jumlah%20pengguna%20internet,jiwa%20penduduk%20Indonesia%20tahun%202023](https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20(APJII)%20mengumumkan%20jumlah%20pengguna%20internet,jiwa%20penduduk%20Indonesia%20tahun%202023). *Jam*, 13.35, 25 Maret, 2024.

atau dikenal juga dengan istilah ponsel atau telepon genggam dan juga komputer yang berkembang menjadi laptop. Dengan berkembangnya ponsel dan juga laptop membuat

manusia dapat dengan mudah membawa alat atau perangkat yang dapat menggunakan internet ke mana – mana. Perkembangan tersebut menimbulkan sebuah tatanan dunia baru yang menjadi tempat untuk melakukan interaksi – interaksi yang dapat dilakukan oleh setiap orang yang berada di mana pun selama memiliki jaringan internet. Dunia tersebut dikenal dengan sebutan dunia maya atau dikenal juga dengan sebutan *cyberspace*. Untuk melindungi hak yang dimiliki oleh setiap orang yang berada di dalam dunia maya diperlukan sebuah aturan yang berguna untuk mengatur setiap interaksi antar manusia yang terjadi di dalam dunia maya. Kemunculan dari internet dan berkembangnya teknologi tersebut memberikan banyak dampak perubahan ke dalam kehidupan masyarakat. Dampak yang diberikan berupa dampak positif dan dampak negatif yang saling berhubungan. Dampak positif yang diberikan dari perkembangan teknologi dan internet adalah kemudahan dalam memberi dan mendapatkan informasi, kemudahan dalam melakukan hubungan dengan orang lain, meningkatkan kesejahteraan dan peradaban dari manusia.³ Namun seperti pedang bermata dua selain memberikan dampak positif bagi kehidupan masyarakat, perkembangan teknologi juga memberikan dampak negatif dalam kehidupan masyarakat, seperti terjadinya kejahatan dengan menggunakan teknologi sebagai sarana maupun tujuan dari tindak kejahatan yang dilakukan.⁴

Tindak kejahatan yang berkembang dalam dunia maya ialah tindak kejahatan *malware*, *hacking*, dan *phising*. *Hacking* merupakan perbuatan tanpa hak dalam mengakses sistem komputer atau sistem elektronik orang lain. Untuk melakukan kejahatan *hacking* seseorang memerlukan sebuah keahlian dalam penguasaan komputer mengenai sistem *software* ataupun *hardware*. *Phising* adalah sebuah kegiatan pengelabuan yang dengan tujuan mendapatkan *username* dan kata sandi dari pengguna komputer dengan membuat sebuah situs palsu yang pada umumnya menjerat para pengguna dari *online banking*. *Malware* adalah sebuah perangkat lunak atau program yang dibuat dengan tujuan mencari kelemahan dari sebuah sistem komputer. *Malware* dibuat agar dapat bekerja dan menyebar dalam jaringan tanpa memerlukan bantuan dari penggunanya. Asal kata *malware* ialah *malicious* yang memiliki arti niat jahat, dan *software* yang diartikan sebagai perangkat lunak. Salah satu jenis *malware* yang digunakan

³ Abdul Wahid, dan Mohammad Labib. *Kejahatan Mayantara (Cyber Crime)*. Rafika Aditama: Bandung, 2005, hal 7.

⁴ Abdul Wahid, dan Mohammad Labib. *Ibid*, hal 8.

untuk melakukan kejahatan adalah *ransomware*. *Ransomware* merupakan istilah yang berasal dari kata *ransom* (Bahasa Inggris) yang jika diubah ke dalam Bahasa Indonesia memiliki arti sebagai tebusan. Sementara kata *ware* dalam *ransomware* adalah singkatan yang diambil dari

kata *software* yang diartikan sebagai perangkat lunak. Maka dapat disimpulkan bahwa arti dari kata *ransomware* adalah perangkat lunak yang bertujuan untuk meminta tebusan. Secara keseluruhan *ransomware* memiliki arti sebagai sebuah perangkat lunak yang digunakan untuk melakukan penguncian data sehingga data tersebut tidak dapat diakses dengan tujuan untuk meminta sebuah tebusan.

Tercatat bahwa pada tahun 2019 di Indonesia telah terjadi suatu kejahatan dengan menggunakan virus *malware* yang berjenis *ransomware* yang telah menyerang Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais.⁵ Setelah terjadi serangan dari *ransomware* tersebut kedua rumah sakit yang bersangkutan tidak dapat melakukan kegiatan dalam melayani pasien yang hadir saat itu karena rumah sakit tidak dapat melakukan akses terhadap data – data kesehatan pasien yang terdapat dalam perangkat lunak atau komputer yang terdapat di rumah sakit, selain tidak dapat melakukan akses atas data kesehatan pasien rumah sakit dan pasien tidak dapat melakukan transaksi pembayaran karena pihak rumah sakit tidak dapat melihat data dari pengobatan yang telah diterima oleh pasien.⁶ Setelah memasukkan virus *ransomware* ke dalam jaringan sistem rumah sakit, pelaku lalu melakukan penguncian data atas sistem jaringan komputer rumah sakit dan pelaku meminta tebusan berupa sejumlah uang dalam bentuk uang digital (*bitcoin*) sebagai ganti dari akses atas jaringan komputer rumah sakit. Pada kejadian ini tidak menyebutkan tindakan rumah sakit dalam melakukan penyelesaian dari tindak kejahatan yang telah terjadi kepada kedua rumah sakit yang bersangkutan. Selain itu dua dalam berita juga tidak menyebutkan adanya tindakan atau usaha untuk melakukan laporan penindakan kepada aparat penegak hukum untuk menindak lanjuti kejadian yang telah terjadi. Pada tahun yang sama selain kasus yang menimpa 2 rumah sakit tersebut, di Indonesia terjadi juga tindak kejahatan *ransomware* yang dilakukan oleh seorang warga negara Indonesia dengan inisial BBA. BBA melakukan kejahatannya dengan menggunakan virus *ransomware* selama 5 tahun

⁵ Lesthia Kertopati, *Dua Rumah Sakit di Jakarta Kena Serangan Ransomware* WannaCry, <https://www.cnnindonesia.com/teknologi/20170513191519-192-214642/dua-rumah-sakit-dijakarta-kena-serangan-ransomware-wannacry> , jam, 19.01, 30 September, 2023.

⁶ Nudirman Munir. *Ibid* hal 5..

dan menargetkan sebuah perusahaan di Amerika. Kejahatan yang dilakukan oleh BBA ini telah berhasil mendapatkan keuntungan dengan meminta uang tebusan berupa uang elektronik hingga sebanyak 300 *bitcoin* atau setara dengan 31,5 Miliar.⁷ Kejadian terbaru yang terjadi di

Indonesia pada akhir Juni tahun 2024 pusat data nasional Indonesia terkena serangan *ransomware* dan meminta uang tebusan sebesar 8 juta USD atau setara dengan 131 miliar rupiah, kejadian ini menyebabkan terganggunya situs pemerintah dan tidak dapat diaksesnya beberapa situs pemerintah baik oleh instansi pemerintah maupun oleh masyarakat Indonesia, di perkirakan 210 instansi pemerintah pusat dan daerah terkena dampak dari serangan ransomware ini.⁸ Kejahatan serangan *ransomware* tersebut tidak hanya terjadi di Indonesia saja, hal serupa juga pernah terjadi di negara – negara lain seperti serangan *ransomware* yang terjadi pada awal tahun 2021 di Amerika Serikat. Kejahatan *ransomware* ini telah menyerang perusahaan pengepakan daging, perusahaan pipa minyak utama di Amerika Serikat, dan perusahaan Microsoft yang melibatkan sistem email *microsoft exchange*. Dalam kasus tersebut Amerika Serikat melakukan pembayaran uang tebusan kepada pelaku untuk mendapatkan kode akses agar dapat melakukan akses terhadap jaringan komputer yang telah di kunci. Karena melakukan pembayaran atas tebusan untuk mendapatkan akses atas komputer tersebut perusahaan Amerika Serikat ini telah mengalami kerugian sebesar US\$ 590 juta atau sebanyak 8.3 triliun rupiah.⁹ Serangan ini dilakukan dengan melakukan pembobolan jaringan entitas lalu mengenkripsi data perusahaan yang menjadi target serangan dan setelah berhasil data – data yang telah dienkripsi dikunci sehingga pemilik data tidak dapat melakukan akses atas data tersebut.

Berdasarkan penjelasan dan juga contoh kasus yang telah dipaparkan di atas maka penelitian ini akan membahas mengenai **“Kejahatan Pemerasan Menggunakan Virus *Ransomware* Dikaitkan Dengan Kejahatan ITE”**.

⁷ Nur Rohmi Aida, Sari Hardiyanto, *Pemuda Sleman Berhasil Retas Perusahaan Amerika dengan Ransomware, Apa Itu?* <https://www.kompas.com/tren/read/2019/10/27/191300865/pemuda-sleman-retas-perusahaanamerika-dengan-ransomware-apa-itu-?page=all> .

⁸ Team CNN Indonesia, “210 Instansi Pusat dan Daerah Kena Dampak Peretasan PDN,” <https://www.cnnindonesia.com/teknologi/20240624152147-192-1113476/210-instansi-pusat-dan-daerah-kenadampak-peretasan-pdn>, jam 22.20

⁹ Novina Putri Bestari, *Ngeri! Virus Ransomware Makan Korban, Rampok Rp 8,3 Triliun*, <https://www.cnbcindonesia.com/tech/20211027062322-37-286775/ngeri-virus-ransomware-makan-korbanrampok-rp-83-triliun> , Jam, 18.06, 30 September, 2023.

1.2 Rumusan Masalah

Berdasarkan latar belakang permasalahan diatas, maka dapat dirumuskan beberapa masalah, yaitu:

-
1. Bagaimanakah UU ITE mengatur pertanggungjawaban pidana pelaku tindak pemerasan dengan menggunakan virus *ransomware* kepada orang yang berada di luar wilayah Negara Indonesia?
 2. Upaya apa yang dapat dilakukan oleh korban dari serangan *ransomware*?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk :

1. Mengetahui kendala apa saja yang terjadi di lapangan dalam mengatasi pelaku tindak kejahatan siber.
2. Untuk mengetahui bagaimana aparat penegak hukum dapat mengatasi hambatan-hambatan yang ada saat melakukan penyidikan atas tindak kejahatan siber.

1.4 Metode Penelitian

Metode penelitian yang digunakan dalam penelitian hukum ini adalah dengan menggunakan jenis penelitian yuridis normatif dengan melihat Undang - Undang No. 1 Tahun 2024 Tentang Perubahan Kedua Undang – Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang – Undang No 19 Tahun 2016 Tentang Perubahan Atas Undang – Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang – Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, dan Kitab Undang – Undang Hukum Pidana. Penelitian ini dilakukan dengan cara seksama untuk mencapai tujuan penelitian yaitu mengetahui perlindungan hukum untuk korban kejahatan *ransomware* dan memberikan kepastian hukum kepada masyarakat terutama dalam tindak kejahatan *ransomware* dengan cara mencari bahan-bahan berupa jurnal/berita/artikel yang berhubungan dengan kejahatan *ransomware*, dan menganalisis Undang – Undang No 19 Tahun 2016 Tentang Perubahan Atas Undang – Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi

Elektronik hingga mendapatkan kesimpulan dan menyusunnya menjadi sebuah laporan.¹⁰ Bahan Hukum Primer yang akan digunakan adalah Kitab Undang – Undang Hukum Pidana, Undang – Undang No. 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang – Undang No. 11 Tahun 2008, Undang - Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Undang - Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas

Undang - Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Sumber hukum primer ini akan didukung dengan adanya tambahan dari sumber hukum sekunder berupa buku/artikel hukum/jurnal hukum yang berhubungan dengan tindak kejahatan *cybercrime*, *malware*, kepastian hukum pidana, *ransomware*.

1.5 Sistematika Penulisan

Bab 1 PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang dilakukannya penelitian atas kepastian hukum demi melindungi korban kejahatan *ransomware*, rumusan masalah yang akan di bahas dalam penelitian mengenai *ransomware* dan Undang – Undang Informasi dan Transaksi Elektronik yang akan dilakukan, tujuan dan kegunaan penelitian, tinjauan pustaka, metode penelitian, dan sistematika penulisan yang digunakan.

Bab 2 KAJIAN TENTANG PENGGUNAAN VIRUS UNTUK PEMERASAN

Bab ini akan berisi mengenai penanggulangan hukum atas tindak kejahatan *ransomware*, selain itu perlindungan hukum atas korban dari tindak kejahatan *ransomware*. Akan berisi mengenai pembahasan mengenai Undang – Undang Informasi dan Transaksi Elektronik, dan peraturan lain yang pada perkembangannya akan digunakan untuk memberikan perlindungan kepada korban kejahatan *ransomware*.

Bab 3 KEJAHATAN INFORMASI DAN TRANSAKSI ELEKTRONIK

Bab ini berisi mengenai kejahatan – kejahatan terhadap jaringan komputer yang diatur dalam Undang – Undang No. 1 Tahun 2024 Tentang Perubahan Kedua atas Undang - Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan penanggulangan atas kejahatan *ransomware* menurut Undang – Undang No. 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang - Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, dan

¹⁰ Soerjono Soekanto dan Sri Mamudji. *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, PT Raja Grafindo Persada: Jakarta, 2006, hal. 13-14.

Kitab Undang - Undang Hukum Pidana sehingga dapat memberikan kepastian hukum bagi masyarakat luas, serta mengenai perluasan wilayah hukum negara.

Bab 4 Pembahasan

Bab akan membahas hasil dari penelitian yang telah dilakukan atas perlindungan hukum untuk korban dari tindak kejahatan *ransomware* dan kepastian hukum atas Undang – Undang Informasi dan Transaksi Elektronik sehingga tidak menimbulkan adanya kerancuan dalam penerapan dari undang – undang yang bersangkutan.

Bab 5 Kesimpulan dan Saran

Pada bab ini penulis menyampaikan kesimpulan dari hasil penelitian hukum yang dilakukan mengenai kejahatan pemerasan menggunakan virus *ransomware* dikaitkan dengan kejahatan ITE berdasarkan Undang - Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi elektronik dan Kitab Undang - Undang Hukum Pidana, Undang – Undang No. 19 tahun 2016 Tentang Perubahan Atas Undang – Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang – Undang No. 1 Tahun 2024 Tentang Perubahan Kedua Undang – Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, dan Kitab Undang – Undang Hukum Pidana.