ANALISIS DAN DETEKSI *MALWARE* PADA PROTOKOL JARINGAN MENGGUNAKAN METODE *MALWARE* ANALISIS DINAMIS DAN *MALWARE* ANALISIS STATIS

SKRIPSI

Oleh
Vicram Renondo Sianipar
190210066

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
TAHUN 2023

ANALISIS DAN DETEKSI *MALWARE* PADA PROTOKOL JARINGAN MENGGUNAKAN METODE *MALWARE* ANALISIS DINAMIS DAN *MALWARE* ANALISIS STATIS

SKRIPSI

Untuk memenuhi salah satu syarat
memperoleh gelar sarjana

Oleh
Vicram Renondo Sianipar
190210066

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
TAHUN 2023

SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini saya:

Nama	: Vicram Renondo Sianipar
NPM	: 190210066
Fakultas	: Teknik dan Komputer
Program Studi	: Teknik Informatika

Menyatakan bahwa **"Skripsi"** yang saya buat dengan judul:

ANALISIS DAN DETEKSI *MALWARE* PADA PROTOKOL JARINGAN MENGGUNAKAN METODE *MALWARE* ANALISIS DINAMIS DAN *MALWARE* ANALISIS STATIS

Adalah hasil karya sendiri dan bukan "duplikasi" dari karya orang lain. Sepengetahuan saya, didalam naskah Skripsi ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip didalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam naskah Skripsi ini dapat dibuktikan terdapat unsur-unsur PLAGIASI, saya bersedia naskah Skripsi ini digugurkan dan gelar akademik yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundangundangan yang berlaku.
Demikian pernyataan ini saya buat dengan sebenarnya tanpa ada paksaan dari siapapun.

Batam, 27 Juli 2023

Vicram Renondo Sianipar
190210066

ANALISIS DAN DETEKSI *MALWARE* PADA PROTOKOL JARINGAN MENGGUNAKAN METODE *MALWARE* ANALISIS DINAMIS DAN *MALWARE* ANALISIS STATIS

SKRIPSI

Untuk memenuhi salah satu syarat
Guna memperoleh gelar sarjana

Oleh:
Vicram Renondo Sianipar
190210066

Telah disetujui oleh Pembimbing pada tanggal
Seperti tertera dibawah ini
Batam, 27 Juli 2023

Hotma Pangaribuan, S.Kom., M.SI
Pembimbing

ABSTRAK

Malware (perangkat lunak berbahaya) telah menjadi ancaman serius bagi keamanan jaringan dan komputer, dan terus mengalami perkembangan yang kompleks. Untuk menghadapi ancaman ini, metode analisis malware telah menjadi fokus utama dalam penelitian keamanan komputer. Dalam penelitian ini, kami mengusulkan pendekatan gabungan berdasarkan analisis dinamis dan analisis statis untuk mendeteksi malware yang menargetkan protokol jaringan. Pertama, kami melakukan analisis malware secara dinamis dengan menjalankan sampel malware pada lingkungan terkontrol dan memantau perilaku eksekusinya. Kami merekam berbagai aktivitas malware, termasuk perubahan sistem, koneksi jaringan, dan upaya menyembunyikan diri. Dari analisis dinamis ini, kami mendapatkan wawasan tentang perilaku malware yang dapat membantu mengidentifikasi tindakan jahatnya. Selanjutnya, kami melakukan analisis statis dengan mengamati kode sumber atau file eksekusi malware tanpa menjalankannya. Teknik ini memungkinkan kami untuk menganalisis struktur dan karakteristik file secara mendalam. Kami menggunakan teknik analisis statis seperti pengurai kode, analisis tanda tangan, dan pembandingan hash untuk mengklasifikasikan file sebagai malware atau non-malware. Selanjutnya, kami mengintegrasikan hasil analisis dinamis dan analisis statis untuk meningkatkan deteksi malware. Dengan memadukan informasi dari kedua metode analisis, kami dapat memperoleh pemahaman yang lebih lengkap tentang malware yang ditargetkan pada protokol jaringan tertentu. Ini membantu dalam mendeteksi varian malware yang sebelumnya tidak diketahui dan meningkatkan akurasi deteksi secara keseluruhan. Untuk menguji keefektifan pendekatan kami, kami melakukan serangkaian uji coba menggunakan berbagai sampel malware yang ada dan mengamati kinerja sistem deteksi kami. Hasil uji coba menunjukkan bahwa pendekatan gabungan kami berhasil mendeteksi dan mengidentifikasi malware pada protokol jaringan dengan tingkat keakuratan yang tinggi. Penelitian ini memberikan kontribusi penting dalam memperkuat pertahanan keamanan jaringan terhadap serangan malware. Dengan menggabungkan analisis dinamis dan analisis statis, sistem deteksi kami memiliki potensi untuk mengenali dan mengatasi ancaman malware masa depan dengan lebih efektif.

Kata Kunci: Protokol Jaringan; Malware; Analisis Dinamis; Analisis Statis

ABSTRACT

Malware (malicious software) has become a serious threat to network and computer security, and continues to undergo complex development. To deal with this threat, malware analysis methods have become a major focus in computer security research. In this study, we propose a combined approach based on dynamic analysis and static analysis to detect malware targeting network protocols. First, we perform dynamic malware analysis by running malware samples in a controlled environment and monitoring their execution behavior. We recorded various malware activities, including system changes, network connections, and concealment attempts. From this dynamic analysis, we gain insights into the malware's behavior that can help identify its malicious actions. Next, we perform static analysis by observing the source code or executable file of the malware without running it. This technique allows us to analyze the structure and characteristics of the file in depth. We use static analysis techniques such as code parsing, signature analysis, and hash comparisons to classify files as malware or non-malware. Furthermore, we integrated the results of dynamic analysis and static analysis to improve malware detection. By combining information from both analysis methods, we were able to gain a more complete understanding of malware targeted at specific network protocols. This helps in detecting previously unknown malware variants and improves the overall detection accuracy. To test the effectiveness of our approach, we conducted a series of trials using various existing malware samples and observed the performance of our detection system. Experimental results show that our combined approach can successfully detect and identify malware on network protocols with a high degree of accuracy. This research makes an important contribution to strengthening network security defenses against malware attacks. By combining dynamic analysis and static analysis, our detection system has the potential to recognize and address future malware threats more effectively.

Keywords: Network Protocol; Malware; Dynamic Analysis; Static Analysis

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas segala berkat dan anugerahNya, sehingga penulis dapat menyelesaikan skripsi ini yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika di Universitas Putera Batam.

Dengan segala keterbatasan, penulis juga menyadari bahwa sksripsi inin takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terimakasih kepada:

1. Ibu Nur Elfi Husda, S.Kom., M.SI., selaku Rektor Universitas Putera Batam
2. Bapak Welly Sugianto, S.T., M.M., selaku Dekan Fakultas Teknik dan Komputer di Universitas Putera Batam
3. Bapak Andi Maslan, S.T., M.SI., selaku Ketua Program Studi Teknik Informatika di Universitas Putera Batam
4. Bapak Hotma Pangaribuan, S.Kom., M.SI., selaku Pembimbing Skripsi pada Program Studi Teknik Informatika di Universitas Putera Batam
5. Bapak Rahmat Fauzi, S.Kom., M.Kom., selaku Pembimbing Akademik pada Program Studi Teknik Informatika di Universitas Putera Batam
6. Seluruh Dosen dan Staff Universitas Putera Batam yang telah memberikan pengetahuan selama perkuliahan
7. Kedua Orangtua yang selalu mendoakan, mendukung, memberikan kasih sayang dan juga menyemangati penulis untuk menyelesaikan perkuliahan S1 ini

8. Zefly Haposan Gultom, S.Kom, selaku Staff *IT* di PT Nok Precision Component Batam yang memberikan izin penelitian ini
9. Almita Rumiris Sianipar, S.S, selaku Kakak yang selalu mendoakan serta memberikan masukan kepada peneliti
10. Erich Alamsyah Sianipar S.T, selaku Abang yang selalu mendoakan serta memberikan semangat kepada peneliti
11. Immanuel Sianipar selaku Adek yang turut serta mendoakan peneliti
12. Suwanda S.Kom, selaku Abang senior yang meluangkan waktunya dan juga memberikan masukan terhadap peneliti
13. Seluruh pihak yang telah banyak membantu dalam menyelesaikan penelitian ini yang tidak dapat penulis sebutkan satu persatu.

Batam, 27 Juli 2023

Vicram Renondo Sianipar

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan di dunia *IT* telah mengubah dunia secara drastis. Inovasi yang cepat dalam komputer, telekomunikasi, dan internet telah menghubungkan orang-orang di seluruh dunia. Peralatan pintar, seperti *smartphone*, telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari. *Internet of Things* (IoT) memungkinkan pengendalian perangkat melalui jaringan, sementara kecerdasan buatan (AI) mendorong kemajuan di bidang seperti otomatisasi, pengenalan suara, dan analisis data yang canggih. Teknologi baru seperti *realitas virtual* (VR) dan *augmented reality* (AR) memberikan pengalaman yang mendalam dan imersif. Namun, perkembangan ini juga memunculkan tantangan baru dalam hal privasi data, keamanan siber, dan kesenjangan teknologi.

Dengan pesatnya perkembangan teknologi keamanan siber pun menjadi tantangan dan masalah baru pada saat ini. Keamanan jaringan melawan *malware* menjadi penting dalam menghadapi ancaman yang terus berkembang di dunia digital saat ini. *Malware*, singkatan dari *malicious software*, merujuk pada perangkat lunak berbahaya yang dirancang untuk merusak atau mencuri data pengguna tanpa izin. Serangan *malware* dapat mengakibatkan kerugian finansial, kehilangan data berharga, atau bahkan merusak reputasi perusahaan. Organisasi dan pengguna perlu mengadopsi langkah-langkah keamanan yang tepat untuk

melindungi jaringan mereka. Ini melibatkan penggunaan perangkat lunak antivirus yang *up-to-date, firewall* yang kuat, pendidikan dan kesadaran pengguna, pembaruan sistem secara teratur, dan kebijakan keamanan yang ketat. Upaya yang berkelanjutan diperlukan untuk menghadapi ancaman *malware* yang terus berkembang dan menjaga integritas jaringan.

Perusahaan swasta dan instansi lain sudah mulai mengambil langkah strategis tentang kemanan jaringan dan data pada perusahan mereka. Salah satunya PT Nok Precision Component Batam (PT. NPCB) merupakan salah satu perusahaan yang bergerak dalam bidang produksi dan pengelolaan *Hard Disk, Drive, Top Cover* yang terletak diwilayah Muka Kuning Batam. Seiring dengan perkembangan teknologi, PT Nok Precision Component Batam juga mengalami perkembangan yang cukup pesat dengan penggunaan sistem yang terkomputerisasi. Perkembangan teknologi yang canggih, proses pengiriman data tidak bias terlepas dari penggunaan jaringan komputer, karena penggunaan jaringan komputer dalam pengiriman data yang efisien dan efektif.

Setiap komputer yang terhubung dengan jaringan komputer memiliki resiko akan terkenanya serangan *malware,* begitu juga dengan komputer-komputer yang ada di PT Nok Precision Component Batam. Karena itu, untuk efisien dan harusnya pembagian data serta pengiriman data, maka setiap komputer yang terhubung dengan jaringan komputer. Sehingga menyebabkan mudahnya serangan malware yang terjadi di komputer-komputer yang terhubung dalam jaringan tersebut.

Malware merupakan perangkat lunak yang digunakan untuk meretas atau merusak sistem didalam komputer. Saat ini penyebaran *malware* sangat mudah,

baik melalui flashdisk, iklan pada *website*, dan media lainnya. Hal itulah yang menyebabkan tindakan kejahatan seperti pencurian data, internet banking, kartu kredit, dan lain sebagainnya. Oleh karena itu, ada suatu bidang yang menangani tindakan kejahatan itu, yaitu forensik digital. Salah satu tahapannya yaitu melakukan analisis terhadap barang bukti digital, dalam hal ini adalah *malware*. Banyak ragam dari *malware* yaitu *Virus, Trojan, Worm, Adware, Spyware, Ransomware, Rootkit, Keylogger, Botnet, Fileless Malware*. Yang saat ini sangat popular adalah serangan *Ransomware*. *Ransomware* adalah jenis khusus *malware* yang bertujuan untuk mengunci atau mengenkripsi data pada sistem komputer yang terinfeksi. Setelah data terkunci, penyerang meminta pembayaran tebusan (*ransom*) dari korban agar mereka dapat mendapatkan kunci dekripsi untuk mengembalikan akses ke data mereka (Manoppo et al., 2020).

Ransomware dapat menyebar melalui metode yang sama seperti *malware* lainnya, seperti melalui email phishing, situs *web* yang terinfeksi, atau eksploitasi kerentanan dalam sistem operasi atau perangkat lunak. Setelah ransomware mengenkripsi data, korban sering diberi tahu melalui pesan tebusan yang menuntut pembayaran dalam bentuk mata uang digital, seperti *Bitcoin*.

Pembayaran tebusan tidak menjamin bahwa data akan dikembalikan, dan dalam beberapa kasus, bahkan setelah pembayaran, data mungkin tetap terenkripsi atau bahkan dihapus. *Ransomware* telah menjadi ancaman yang semakin serius, dengan serangan besar seperti itu yang menyebabkan kerugian finansial yang signifikan dan mengganggu operasi banyak organisasi di seluruh dunia.

Menurut (Wahidin et al., 2022) Indonesia menempati posisi ketiga di Asia Tenggara, dengan jumlah serangan *ransomware* terbanyak, sebesar 14 laporan serangan *ransomware*. Menurut catatan Palo Alto Networks, pelaku ancaman menggunakan taktik yang lebih agresif untuk menekan organisasi, dengan jumlah gangguan 20 kali lebih banyak dibandingkan 2021, menurut kasus penanganan insiden Unit 42. Temuan ini selaras dengan laporan Badan Siber dan Sandi Negara (BSSN), yang menyebut bahwa *ransomware* dan pembobolan merupakan jenis serangan siber paling umum di 2022. Menurut BSSN, mereka menyumbang 50 persen dari seluruh serangan siber yang dilaporkan di Indonesia pada tahun 2022 (Wahidin et al., 2022).

Gangguan ini biasanya dilakukan lewat panggilan telepon dan email yang menargetkan individu tertentu, seringkali di *C-suite* atau pelanggan, untuk mendesak agar membayar permintaan uang tebusan. Untuk melindungi diri dari *malware* dan *ransomware*, penting untuk menjaga sistem operasi dan perangkat lunak yang terinstal tetap diperbarui, menggunakan solusi keamanan yang terkini, waspada terhadap *email* yang mencurigakan atau tautan yang tidak diketahui, serta melakukan pencadangan data secara teratur sebagai langkah pencegahan utama.

Analisa *malware* secara umum dapat dilakukan dengan dua metode, yaitu *Dynamic Analysis*, dan *Static Analysis*. Meskipun tujuan dari kedua metode tersebut sama yaitu untuk menjelaskan tentang bagaimana sebuah *malware* bekerja tetapi dalam proses analisa kedua metode tersebut sangatlah berbeda baik dari segi *tools*, waktu dan kemampuan. *Dynamic analysis* dilakukan dengan mengeksekusi contoh *malware* untuk kemudian dipelajari perilaku yang ditimbulkan oleh *malware*

tersebut. Berbeda pula dengan *static analysis* yang pada saat proses analisanya tidak mengeksekusi contoh *malware* melainkan dengan membongkar *source code malware* lalu mempelajari dan memahami kode tersebut (Manoppo et al., 2020)

Dynamic Analysis dapat dilakukan menggunakan dua cara yaitu manual dan atau menggunakan tool analisa otomatis yaitu *cuckoo sandbox. Cuckoo sandbox* dapat melakukan analisa *malware* secara otomatis dan menampilkan informasi-informasi yang dilakukan oleh sampel *malware*. *Cuckoo Sandbox* merupakan *tool* analisa *malware* dan dapat memberikan beberapa informasi mengenai *malware* yang sedang berjalan dalam lingkungan yang terisolasi (Manoppo et al., 2020).

Malware Analysis Static tidak sama dengan *Malware Analysis Dynamic*, dalam metode analisis statis ini file *malware* tidak akan diaktifkan secara langsung melainkan diteliti serta dianalisis terhadap kode sumber yang dituliskan didalam program *malware* dengan menggunakan tahapan pembedahan terhadap program *malware* tersebut, sehingga informasi yang didapatkan lengkap dan bisa memberikan gambaran detail tentang mekanisme kerja *malware* tersebut secara keseluruhan (Manoppo et al., 2020).

Berdasarkan dampak yang dapat disebabkan oleh *malware* jenis *Ransomware* bagi pengguna dan protokol jaringan komputer yang dapat menghambat kinerja PT Nok Precision Component Batam, maka peneliti termotivasi untuk melakukan penelitian yang berjudul **"ANALISIS DAN DETEKSI *MALWARE* PADA PROTOKOL JARINGAN MENGGUNAKAN METODE *MALWARE* ANALISIS DINAMIS DAN *MALWARE* ANALISIS STATIS".**

1.2 Identifikasi Masalah

Sesuai yang dijabarkannya latar belakang masalah, adapun identifikasi masalah pada penelitian ini yaitu:

1. Kesulitan melakukan mitigasi dan pencegahan *ransomware* yang mengenkripsi data pada sistem komputer yang terinfeksi, membuatnya tidak dapat diakses oleh pemiliknya. Ini dapat menyebabkan kerugian finansial dan operasional yang signifikan bagi organisasi, karena data yang terenkripsi mungkin berisi informasi penting, termasuk data pelanggan, data bisnis, atau data keuangan.
2. Kurangnya keamanan jaringan sehingga mudah untuk diserang dari infrastruktur dan tenanga khusus analis dan team kemana siber pada perusahaan.
3. Perkembangan yang cepat serta varian dari jenis *ransomware* yang selalu berkemangan dengan teknik yang berbeda beda dari tahun ke tahun.

1.3 Batasan Masalah

Berdasarkan identifikasi masalah diatas, dan penelitian ini tidak terlalu luas cakupannya maka peneliti hanya membatasi masalah sebagai berikut:

1. Perangkat yang digunakan adalah *virtual machine* dengan sistem operasi *windows* 7 yang dijalankan dengan *virtualbox*.
2. Analisis yang akan dilakukan adalah dasar analisis statis.
3. Analisis dinamis dilakukan menggunakan *cuckoo sandbox* dan akan menghasilkan data *behaviour* analisis dan *process tree*.
4. *Ransomware* yang akan dianalisis hanya jenis *Petya* dan *Gandcrab*.

1.4 Rumusan Masalah

Berdasarkan batasan masalah yang telah dijabarkan diatas, adapun rumusan masalah dari penelitian ini yaitu;

1. Bagaimana cara menyiapkan *environment* khusus untuk melihat jenis *Ransomware Petya* dan *Grandcrab*?
2. Bagaimana cara melakukan analisis statis dengan benar?
3. Bagaimana cara melakukan analisis dinamis menggunakan *Cuckoo Sandbox*?
4. Bagaimana melakukan mitigasi dan pemetaan evolusi dari kedua metode analisis tersebut?

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijabarkan diatas, adapun tujuan dari penelitian ini yaitu;

1. Untuk menyiapkan *environment* khusus untuk melihat jenis *Ransomware Petya* dan *Grandcrab*.
2. Untuk melakukan analisis statis dengan benar.
3. Untuk melakukan analisis dinamis menggunakan *Cuckoo Sandbox*.
4. Untuk melakukan mitigasi dan pemetaan evolusi dari kedua metode analisis tersebut.

1.6 Manfaat Penelitian

Hasil dari penelitian yang dilakukan penulis berharap kiranya dapat bermanfaat bagi berbagai pihak, adapun manfaat dari penelitian ini yaitu;

1.6.1 Manfaat Teoritis

Penulis berharap baik secara langsung maupun tidak langsung penelitian ini dapat bermanfaat pada berbagai pihak, yaitu diantaranya:

1. Menambah wawasan dalam bidang menganalisa jenis serangan *malware* khususnya *ransomware* jaringan menggunakan metode analisis statis dan dinamis.
2. Menambah keahlian dalam bidang menganalisa, mitigasi serangan ataupun ancaman *ransomware* pada jaringan menggunakan metode *malware* analisis statis dan dinamis.
3. Mengetahui keamanan jaringan yang dapat diserang orang yang tidak bertanggung jawab.

1.6.2 Manfaat Praktis

Penulis berharap baik secara langsung maupun tidak langsung penelitian ini dapat bermanfaat pada berbagai pihak, yaitu diantaranya:

1. Bagi Penulis

   Penelitian ini diharapkan dapat menambah dan meningkatkan pengetahuan dalam menganalisa jaringan menggunakan metode *malware* analisis dinamis dan metode *malware* analisis statis.

2. Bagi Mahasiswa

   Penelitian ini diharapkan dapat digunakan sebagai referensi dan sumber pengetahuan pada penelitian selanjutnya.

3. Bagi PT Nok Precision Component Batam

Penelitian ini diharapkan dapat membantu mengetahui kelemahan jaringan komputer dan langkah strategis menanggapi serangan *cybercrime* khususnya *malware* yang dapat mengganggu aktifitas perusahaan.

BAB II

TINJAUAN PUSTAKA

2.1 Teori Dasar

2.1.1 Pengertian Jaringan Komputer

Jaringan Komputer merupakan interaksi antara dua komputer *autonomous* atau lebih, yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless)*. *Autonomous* adalah apabila sebuah komputer tidak melakukan kontrol terhadap komputer lain dengan akses penuh, sehingga dapat membuat komputer lain *restart*, *shutdown*, kehilangan file atau kerusakan sistem. (Sani et al., 2020)

2.1.2 Standar jaringan Komputer

Standar Jaringan Komputer merupakan protokol yang telah disepakati oleh industri jaringan dan disahkan oleh suatu Organisasi Standar.

Dibawah ini merupakan beberapa Organisasi yang concern dengan perkembangan standar teknologi telekomunikasi dan data internasional maupun dari Amerika (Novenzo Ihsana & Maslan, 2020).

1. *Internasional Standards Organization* (ISO).
2. *Internasional Telecommunications Union-Telecommunication Standards Section* (ITU-T).
3. *American National Standards Institute* (ANSI)
4. *Institute of Electrical and Electronics Engineers* (IEEE).
5. *Electronics Industries Association* (EIA)

Selain itu ada juga organisasi yang bersifat forum ilmiah seperti *Frame Relay Forum* dan ATM Forum. Kemudian ada juga organisasi yang berfungsi sebagai agen regulasi, misalnya *Federal Communications Commision* (FCC).

2.1.3 Jenis Jaringan Komputer

Menurut (Santoso et al., 2022) terdapat berbagai jenis jaringan komputer yang umum digunakan dikehidupan sehari-hari, antara lain:

1. *Local Area Network* (LAN)

   Salah satu tipe jaringan komputer yang umum dijumpai adalah *Local Area Network* atau LAN. Jaringan ini dijangkau cenderung kecil dan paling sering diterapkan di beberapa lokasi seperti kantor, sekolah, dan rumah.

2. *Personal Area Network* (PAN)

   Hampir sama seperti LAN, jenis jaringan komputer PAN juga paling sering diterapkan pada gedung perkantoran maupun hunian pribadi. Biasanya, pengguna PAN hanya sebatas keperluan standar seperti menyediakan jaringan internet saja.

3. *Metropolitan Area Network* (MAN)

   Cakupan wilayah yang menerapkan jenis jaringan komputer MAN tentunya lebih besar dibandingkan PAN dan LAN.Pengguna MAN didedikasikan untuk menghubungkan satu jaringan komputer ke komputer lainnya dalam skala kota.

4. *Virtual Private Network* (VPN)

Virtual Private Network merupakan salah satu dari jenis-jenis jaringan komputer yang digunakan ketika seseorang ingin mengakses sebuah situs memakai jaringan pribadi. Biasanya VPN digunakan oleh beberapa pihak yang ingin melindungi situs mereka karena mengandung konten sensitif, sehingga dibutuhkan VPN untuk menyamarkan keberadaan situs tersebut di internet.

5. *Wide Area Network* (WAN)

   Memanfaatkan teknologi yang sangat canggih, jenis jaringan komputer bernama *Wide Area Network* memberikan keuntungan berupa jangkauan area yang sangat luas. Tidak hanya bisa digunakan pada kawasan gedung atau antar kota saja, WAN mampu menjangkau jaringan antar negara hingga benua.

6. Internet

   Internet adalah jaringan global yang menghubungkan jutaan komputer di seluruh dunia. Ia memungkinkan kita untuk berkomunikasi, mencari informasi, dan berbagi data dengan cepat dan efisien. Internet telah mengubah cara kita hidup, bekerja, dan belajar. Dengan akses internet, kita dapat terhubung dengan orang-orang di seluruh dunia, menjelajahi dunia maya, dan mengakses berbagai layanan online. Namun, perlu diingat bahwa penggunaan internet juga perlu dilakukan dengan bijak, dengan menjaga privasi dan keamanan kita. Internet adalah sebuah inovasi yang mendasar dalam era digital kita dan memiliki peran penting dalam perkembangan masyarakat modern (Putra & Maslan, 2022)

2.1.4 TCP/IP

TCP/IP adalah singkatan dari *Transmission Control Protocol/Internet Protocol*. Ini adalah sekumpulan protokol jaringan yang digunakan untuk mengatur komunikasi dan pertukaran data antara perangkat di jaringan komputer.

TCP/IP adalah protokol standar yang digunakan dalam jaringan komputer untuk mentransmisikan data secara efisien dan dapat diandalkan. Protokol ini terdiri dari dua bagian utama yaitu *Transmission Control Protocol* (TCP) dan internet Protocol (IP). TCP bertanggung jawab untuk memastikan pengiriman data yang andal dengan menggunakan mekanisme tanda terima dan pengiriman ulang jika diperlukan. TCP juga mengatur aliran data dan pengontrolan kongesti untuk mencegah kelebihan beban jaringan.

IP adalah protokol yang bertanggung jawab untuk mengarahkan paket data melalui jaringan. IP menentukan alamat tujuan dan sumber paket data, serta memastikan bahwa paket-paket tersebut tiba dengan benar ke tujuan yang dituju. Selain TCP dan IP, TCP/IP juga mencakup protokol lainnya seperti *User Datagram Protocol* (UDP) yang digunakan untuk aplikasi yang membutuhkan transfer data yang lebih cepat tetapi kurang andal (Novenzo Ihsana & Maslan, 2020)

TCP/IP memiliki model lapisan yang terdiri dari empat lapisan: lapisan aplikasi, lapisan transport, lapisan jaringan, dan lapisan fisik. Setiap lapisan memiliki fungsi dan tanggung jawab tertentu dalam proses komunikasi jaringan.

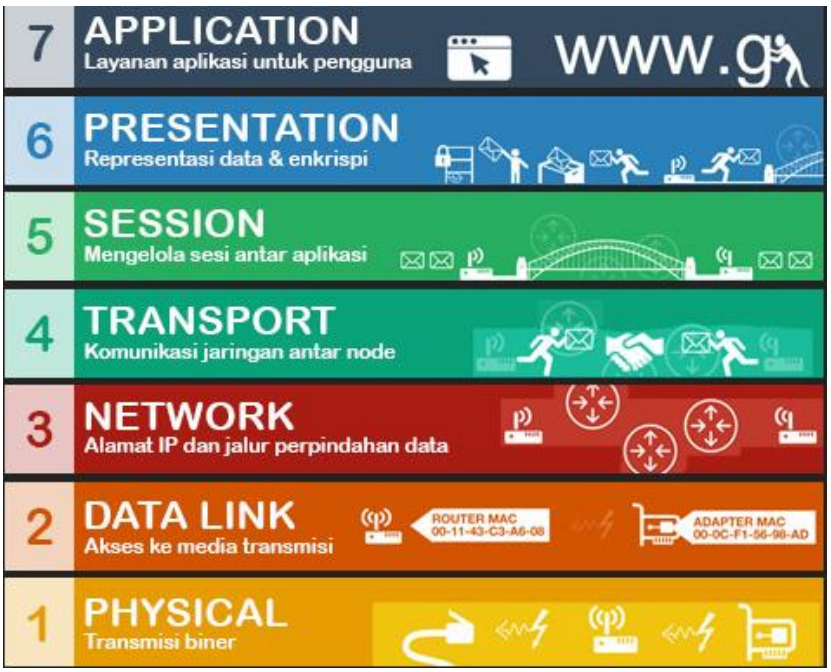
Protokol TCP/IP mendukung berbagai aplikasi seperti email, *browsing web*, transfer file, dan banyak lagi. Hal ini memungkinkan komunikasi yang mulus antara perangkat-perangkat di seluruh jaringan komputer global. Dalam komunikasi

TCP/IP, data dikemas dalam paket-paket yang dikirim melalui jaringan. Setiap paket memiliki header yang berisi informasi seperti alamat sumber dan tujuan, nomor urut, dan checksum untuk memastikan keintegritasan data.

Dengan adopsi yang luas dan menjadi dasar internet saat ini, TCP/IP telah menjadi protokol yang sangat penting dalam menghubungkan perangkat dan memungkinkan pertukaran data di seluruh dunia.

2.1.5 Model OSI Layer

OSI layer merupakan sebagai rujukan agar produk atau *software* yang dibuat dapat bersifat interpolate yang berarti pengguna bisa bekerja sama dengan produk atau sistem tanpa perlu melakukan penanganan secara khusus (Novenzo Ihsana & Maslan, 2020).



Gambar 2. 1 Model OSI Layer
(Sumber Penelitian : 2023)

Berikut merupakan tujuh model OSI layer yang dimana setiap lapisannya memiliki fungsi dan tugas masing-masing.

1. *Application Layer* (Lapisan ke 7)

   Application layer pada OSI merupakan pusat terjadinya suatu interaksi antara pengguna dengan aplikasi yang bekerja menggunakan fungsionalitas sebuah jaringan. Contoh protokolnya adalah HTTP, FTP, dan SMTP.

2. *Presentation Layer* (Lapisan ke6)

   Lapisan Presentation berfungsi sebagai mengidentifikasi sintaks yang dipakai suatu host jaringan untuk berkomunikasi. Contoh protokolnya adalah MIME, TLS, dan SSL.

3. *Session Layer* (Lapisan ke 5)

   Layer Session berfungsi untuk mengendalikan dialog maupun melakukan pengelolaan terhadap koneksi suatu komputer. Contoh protokolnya adalah NFS, RTP, dan SMB.

4. *Transport Layer* (Lapisan ke 4)

   Lapisan transport layer ini memiliki peran untuk menyalurkan bit. Dengan layer ini, data bisa disalurkan dari server menuju ke pengguna tanpa adanya gangguan.

5. *Network Layer* (Lapisan ke 3)

   Layer network pada OSI ini berfungsi mendefinisikan alamt IP sehingga setiap komputer dapat saling terkoneksi dalam satu jaringan.

6. *Data Link Layer* (Lapisan ke 2)

   Fungsi utama dari data link layer merupakan untul memeriksa bila terjadi kesalahan dalam menyalurkan transmisi terhadap bit data. Pada layer ini juga terjadi koreksi kesalahan, pengalamatan hardware pada MAC *address* dan *flow control*.

7. *Physical Layer* (Lapisan pertama)

   Physical layer OSI merupakan lapisan yang bertugas untuk sebagai transmisi terhadap bit data. Jenis sinyalnya pun harus didukung media fisik misalnya kabel, infrared, cahaya biasa, frekuensi radio, dan tegangan listrik. Setelah layer ini menyelesaikan tugasnya, maka akan diteruskan ke layer kedua.

2.2 Teori Khusus

2.2.1 *Malware*

Menurut (Manoppo et al., 2020) *Malware*, singkatan dari *malicious software*, adalah perangkat lunak yang dirancang untuk merusak, mengganggu, atau mengambil alih sistem komputer tanpa izin pengguna. *Malware* dapat memengaruhi berbagai jenis perangkat, termasuk komputer, ponsel, tablet, dan perangkat cerdas lainnya. Berikut adalah beberapa jenis *malware* yang umum ditemui (Novenzo Ihsana & Maslan, 2020):

1. *Virus*

   Menempel pada file atau program dan menyebar saat file atau program tersebut dijalankan. *Virus* dapat merusak data, menghapus file, atau bahkan menghancurkan seluruh sistem.

2. *Worm*

   Menyebar melalui jaringan komputer dan menggandakan diri untuk menyerang perangkat lain. *Worm* dapat memanfaatkan kerentanan keamanan untuk mencuri informasi atau merusak sistem.

3. *Trojan Horse*

   Menyamar sebagai program yang berguna atau mengunduhnya tanpa izin pengguna. *Trojan Horse* dapat membuka pintu belakang pada sistem untuk memungkinkan akses tanpa izin atau mencuri informasi pribadi.

4. *Spyware*

   Mengumpulkan informasi tentang pengguna tanpa sepengetahuannya. Spyware sering kali digunakan untuk mencuri informasi pribadi, seperti kata sandi, data keuangan, atau riwayat penelusuran.

5. *Adware*

   Menampilkan iklan yang tidak diinginkan kepada pengguna. *Adware* biasanya terpasang bersama dengan perangkat lunak gratis atau didistribusikan melalui unduhan tidak sah.

6. *Keylogger*

   Merekam setiap ketukan tombol yang dilakukan pengguna pada perangkat, termasuk kata sandi dan informasi sensitif lainnya. *Keylogger* digunakan untuk mencuri data pribadi.

7. *Ransomware*

   Memblokir akses pengguna ke sistem atau file dengan mengenkripsi data dan meminta tebusan agar data tersebut dikembalikan. *Ransomware* sering

kali mengeksploitasi ketidaktahuan pengguna untuk menyebar (Usharani et al., 2021). Adapun jenis dari *Malware type* ransomware sebagai berikut:

a. *Petya*

Ransomware Petya adalah jenis serangan siber yang mengenkripsi data korban dan meminta tebusan untuk mendapatkan kunci dekripsi. *Petya* pertama kali muncul pada tahun 2016 dan telah mengalami variasi dan modifikasi sejak saat itu. Serangan ini biasanya dimulai dengan mengirimkan email phishing atau memanfaatkan kerentanan perangkat lunak. Ketika sistem terinfeksi, *Petya* mengenkripsi file dan mengunci akses ke sistem tersebut. *Ransomware* ini kemudian menampilkan pesan tebusan yang meminta pembayaran dalam bentuk mata uang digital agar data bisa dikembalikan. *Petya* menjadi salah satu ancaman siber yang serius bagi perusahaan dan pengguna individu, dan mendorong pentingnya keamanan siber yang kuat.

Gambar 2. 2 Contoh Serangan *Ransomware Petya*
(Sumber Penelitian:2023)

b. *Gandcrab*

Gambar 2. 3 Jenis *Ransomware Gandcrab*
(Sumber Penelitian:2023)

GandCrab adalah salah satu jenis *ransomware* yang pertama kali muncul pada tahun 2018. *GandCrab* menyebar melalui berbagai metode, seperti *email phishing*, eksploitasi kerentanan, atau perangkat lunak ilegal. Setelah mengenkripsi file, *GandCrab* menampilkan pesan yang meminta pembayaran tebusan dalam bentuk mata uang *kripto*, seperti *Bitcoin*, untuk mendapatkan kunci dekripsi.

2.2.2 *Virtual Machine*

Virtual Machine (VM) adalah teknologi yang telah merevolusi dunia komputasi modern. Artikel ini akan menjelaskan konsep dasar, manfaat, dan penerapan *virtual machine* dalam berbagai bidang, termasuk pengembangan perangkat lunak, pengujian, dan pengelolaan infrastruktur. VM memungkinkan pengguna untuk menjalankan beberapa sistem operasi dan aplikasi secara bersamaan pada satu mesin fisik, menyediakan lingkungan terisolasi yang aman dan efisien. Dengan menggunakan teknologi seperti *hypervisor*, VM dapat mengalokasikan sumber daya komputer secara dinamis dan memungkinkan

pengguna untuk mengelola dan mengontrol lingkungan virtual (Dewanje & Kumar, 2020).

2.2.3 *Operating System*

Sistem operasi adalah perangkat lunak yang mengelola sumber daya komputer dan menyediakan antarmuka antara pengguna dan perangkat keras. Ia mengendalikan eksekusi program, manajemen memori, akses file, dan koordinasi perangkat keras.

Sistem operasi memungkinkan pengguna untuk menjalankan aplikasi dan berinteraksi dengan komputer secara efisien. Ia juga bertanggung jawab atas keamanan dan perlindungan data. Sistem operasi yang populer termasuk Windows dan Linux. Dalam dunia yang semakin terhubung secara digital, sistem operasi terus berkembang untuk mendukung teknologi baru dan memenuhi kebutuhan pengguna modern (Pan et al., 2020).

2.2.4 *Machine Learning*

Machine learning ransomware analysis adalah sebuah pendekatan yang menggunakan teknik machine learning untuk menganalisis dan mendeteksi *ransomware*. *Ransomware* merupakan jenis *malware* yang bertujuan untuk mengenkripsi data pengguna dan meminta tebusan agar data tersebut dapat dikembalikan. Dalam upaya melawan ancaman ini, para peneliti keamanan dan ahli dalam bidang keamanan informasi telah mengembangkan metode baru yang memanfaatkan kecerdasan buatan.

Pada dasarnya, *machine learning ransomware analysis* melibatkan proses pelatihan algoritma *machine learning* menggunakan data yang dikumpulkan dari

berbagai jenis *ransomware* yang ada. Algoritma ini belajar mengenali pola dan karakteristik khas yang terdapat dalam serangan *ransomware*. Setelah melalui tahap pelatihan, algoritma tersebut dapat digunakan untuk menganalisis dan mendeteksi ancaman *ransomware* baru secara otomatis.

Salah satu keunggulan dari pendekatan ini adalah kemampuannya untuk mengidentifikasi varian *ransomware* yang belum pernah ditemui sebelumnya. Karena *machine learning* dapat mengenali pola dan perilaku yang tidak biasa, algoritma tersebut dapat mengidentifikasi dan mengklasifikasikan *ransomware* baru berdasarkan kesamaan dengan pola yang telah dipelajari. Hal ini memungkinkan untuk mengambil tindakan preventif sebelum *ransomware* tersebut menyebabkan kerusakan yang lebih lanjut (Santoso et al., 2022)

Selain itu, dengan menggunakan *machine learning ransomware analysis*, analisis dan deteksi dapat dilakukan secara real-time. Algoritma dapat diintegrasikan dengan sistem keamanan yang ada, sehingga dapat secara otomatis memonitor aktivitas yang mencurigakan dan merespons dengan cepat ketika terdeteksi ancaman *ransomware*.

Meskipun *machine learning ransomware analysis* memiliki banyak potensi dalam melawan serangan *ransomware*, metode ini juga memiliki tantangan. *Ransomware* terus berkembang dan penyerang dapat mengubah pola serangannya untuk menghindari deteksi. Oleh karena itu, diperlukan pembaruan dan pengembangan terus-menerus dari algoritma *machine learning* untuk tetap efektif dalam menghadapi ancaman yang baru dan berkembang.

Secara keseluruhan, *machine learning ransomware analysis* merupakan pendekatan yang menjanjikan dalam melawan serangan *ransomware*. Dengan menggunakan kecerdasan buatan, metode ini dapat membantu dalam mendeteksi dan melindungi sistem dari ancaman yang semakin kompleks (Rachmat, 2019).

2.3 Tools

2.3.1 Tools Analisis Statis

2.3.1.1 HXD Editor

HXD (Hex Editor) adalah alat perangkat lunak yang digunakan untuk menganalisis dan memodifikasi berkas biner dengan format heksadesimal. Meskipun HXD dapat digunakan dalam analisis malware (Manoppo et al., 2020). Berikut adalah beberapa fitur dan fungsionalitas HXD yang dapat berguna dalam analisis *malware*:

1. Tampilan Heksadesimal

   HXD menyediakan tampilan heksadesimal dari berkas biner, yang memungkinkan pengguna untuk melihat dan menganalisis kode mesin, string, dan struktur data dalam berkas *malware*.

2. Analisis String

   HXD memungkinkan pengguna untuk mencari dan menganalisis string yang ada dalam berkas, yang dapat membantu dalam mengidentifikasi pesan yang terkait dengan *malware*, URL yang digunakan, atau kata kunci lainnya yang relevan.

3. Analisis Struktur Data

   Alat ini memungkinkan pengguna untuk menganalisis dan menginterpretasikan struktur data dalam berkas, seperti *header* file, tabel ekspor dan impor, dan bagian lain yang mungkin relevan dalam analisis *malware*.

4. Modifikasi dan Rekayasa Balik

   HXD dapat digunakan untuk memodifikasi berkas biner dan melihat dampaknya pada perilaku *malware*. Selain itu, HXD dapat membantu dalam rekayasa balik (*reverse engineering*) dengan memahami kode mesin dan aliran eksekusi dalam berkas *malware*.

Namun, perlu diingat bahwa analisis *malware* yang efektif memerlukan pengetahuan mendalam tentang teknik dan taktik *malware* yang terbaru. Selain itu, penggunaan HXD dan alat sejenis lainnya harus dilakukan dengan hati-hati dan memperhatikan aspek hukum serta etika yang terkait dengan analisis *malware*. Disarankan untuk menggunakan HXD sebagai bagian dari pendekatan yang lebih luas dalam analisis *malware* dan mendapatkan bantuan dari ahli keamanan cyber yang berpengalaman.

2.3.1.2 PE Studio

PEStudio adalah alat perangkat lunak yang dapat digunakan untuk menganalisis berkas eksekusi Windows (PE, atau Portable Executable). Meskipun PEStudio dapat digunakan dalam analisis *ransomware* (Manoppo et al., 2020)

PEStudio dapat membantu dalam menganalisis berkas eksekusi untuk mengidentifikasi perilaku yang mencurigakan, tanda-tanda *ransomware*, atau fitur

yang umumnya terkait dengan perangkat lunak berbahaya. Beberapa fitur dan fungsionalitas PEStudio yang dapat berguna dalam analisis *ransomware* meliputi:

1. Identifikasi Fitur Berbahaya

   PEStudio memeriksa berbagai atribut berkas eksekusi, termasuk impor API, string yang mencurigakan, entri registri yang diubah, entri startup yang dicapai, dan tanda-tanda lainnya yang dapat mengindikasikan keberadaan *ransomware*.

2. Penjelajahan *Ressources*

   Alat ini memungkinkan pengguna untuk menelusuri dan menganalisis sumber daya dalam berkas eksekusi, seperti string yang tersembunyi atau pesan-pesan yang terkait dengan *ransomware*.

3. Pemecahan Masalah Eksekusi

   PEStudio dapat membantu mengidentifikasi masalah yang mungkin terjadi saat eksekusi berkas, seperti panggilan fungsi yang mencurigakan, kode yang disisipkan, atau tindakan yang tidak biasa.

4. Analisis Dependensi

   PEStudio dapat membantu dalam melacak dependensi berkas eksekusi dan mengidentifikasi perangkat lunak tambahan atau modul yang terlibat, yang dapat memberikan wawasan tentang perilaku *ransomware* yang potensial.

Penting untuk dicatat bahwa meskipun PEStudio dapat memberikan wawasan dan bantuan dalam menganalisis berkas eksekusi yang mencurigakan, analisis *ransomware* yang efektif memerlukan pengetahuan mendalam tentang teknik dan taktik *ransomware* yang terbaru. Oleh karena itu, disarankan untuk menggunakan

alat ini sebagai bagian dari pendekatan yang lebih luas dalam menganalisis dan melawan ancaman *ransomware*.

2.3.1.3 CFF Explorer

CFF Explorer merupakan perangkat lunak yang digunakan untuk memeriksa dan menganalisis berkas biner, terutama berkas eksekusi Windows (misalnya, EXE dan DLL). CFF Explorer dikembangkan oleh Daniel Pistelli dan memberikan berbagai fitur untuk membantu dalam analisis dan pemahaman struktur berkas biner (Manoppo et al., 2020).

Berikut ini adalah beberapa fitur umum yang dimiliki oleh CFF Explorer:

1. Analisis Berkas

   CFF Explorer memungkinkan pengguna untuk menganalisis berbagai atribut dan struktur dalam berkas biner, termasuk entri ekspor dan impor, tabel relokasi, *header*, dan informasi lainnya yang berkaitan dengan struktur berkas.

2. Penjelajahan *Ressources*:

   Alat ini memungkinkan pengguna untuk menelusuri dan menganalisis berbagai sumber daya (*resources*) yang disertakan dalam berkas, seperti ikon, gambar, string, dll.

3. Pemecahan Masalah Eksekusi:

   CFF Explorer dapat digunakan untuk memeriksa struktur PE (Portable Executable) dari berkas eksekusi dan memeriksa masalah yang mungkin terjadi saat proses eksekusi, seperti dependensi DLL yang hilang atau masalah pemanggilan fungsi.

4. Penambahan Manifest:

   Pengguna dapat menggunakan CFF Explorer untuk menambahkan, mengubah, atau menghapus manifest aplikasi yang terkait dengan berkas biner. Manifest aplikasi adalah file XML yang berisi informasi tentang aplikasi dan persyaratan sistem yang diperlukan.

5. Alat Pemecah Kode (*Disassembler*)

   CFF Explorer menyediakan disassembler yang dapat digunakan untuk menganalisis kode mesin dan mendapatkan pemahaman tentang operasi dan aliran eksekusi program.

CFF Explorer sering digunakan oleh pengembang perangkat lunak, peneliti keamanan, dan profesional TI dalam analisis dan pemecahan masalah berkas eksekusi. Namun, penting untuk menggunakan alat ini dengan bijak dan dengan pemahaman yang baik tentang etika dan legalitas penggunaannya.

2.3.1.4 EXE Info

EXEinfo PE adalah sebuah perangkat lunak yang digunakan untuk melakukan analisis statis pada file *executable* (berkas eksekusi), termasuk juga untuk mengidentifikasi dan menganalisis *malware*. Dengan menggunakan EXEinfo PE, pengguna dapat melihat informasi rinci tentang file eksekusi, seperti *header*, sektor, entri poin, serta fitur-fitur dan fungsi yang terkait. Selain itu, perangkat lunak ini dapat mendeteksi tanda-tanda yang mencurigakan atau karakteristik yang umum ditemukan pada berkas yang berpotensi berbahaya (Manoppo et al., 2020).

Dengan analisis statis yang cermat, EXEinfo PE dapat membantu pengguna untuk mengidentifikasi dan mengklasifikasikan malware serta memahami lebih lanjut tentang fitur dan perilaku berkas eksekusi tersebut.

2.3.1.5 Virustotal

VirusTotal adalah layanan online yang menyediakan pemindaian dan analisis berkas untuk mendeteksi *malware* dan ancaman keamanan lainnya (Manoppo et al., 2020). Layanan ini memungkinkan pengguna untuk mengunggah berkas atau memasukkan URL ke dalam platform, lalu melakukan pemindaian dengan menggunakan berbagai mesin pemindai antivirus dan alat keamanan lainnya. Berikut adalah beberapa fitur dan fungsionalitas VirusTotal:

1. Pemindaian Berkas

   VirusTotal menggunakan berbagai mesin pemindai antivirus terkemuka untuk memeriksa berkas yang diunggah dan mengidentifikasi adanya *malware*, *virus*, *worm*, *trojan*, atau ancaman keamanan lainnya.

2. Pemindaian URL:

   Layanan ini memungkinkan pengguna untuk memeriksa URL dan memvalidasi keamanannya. Ini berguna untuk mengidentifikasi URL yang mencurigakan atau diketahui terkait dengan penipuan, phishing, atau penyebaran *malware*.

3. Deteksi Heuristik

   VirusTotal juga menerapkan teknik deteksi heuristik untuk mengenali ancaman baru yang belum diketahui secara spesifik oleh mesin pemindai

antivirus. Ini membantu dalam mendeteksi ancaman yang tidak terdeteksi oleh mesin pemindai tertentu.

4. Analisis Rinci:

   Setelah pemindaian selesai, VirusTotal memberikan laporan rinci tentang hasil pemindaian berkas atau URL, termasuk informasi tentang deteksi, nama-nama mesin pemindai yang mendeteksi ancaman, dan informasi lain yang relevan.

5. Intelijen Keamanan: VirusTotal juga menyediakan intelijen keamanan yang berisi informasi tentang berkas, URL, dan ancaman terkait lainnya. Pengguna dapat mengakses informasi ini untuk mendapatkan wawasan lebih lanjut tentang ancaman yang terdeteksi.

VirusTotal dapat digunakan oleh pengguna individu, peneliti keamanan, dan organisasi untuk memeriksa dan menganalisis berkas atau URL yang mencurigakan. Layanan ini membantu dalam mendapatkan pemahaman yang lebih baik tentang tingkat keamanan berkas dan URL yang terkait dengan ancaman keamanan.

2.3.2 Tools Analisis Dinamis

2.3.2.1 Virtualbox

VirtualBox adalah perangkat lunak virtualisasi yang populer yang dikembangkan oleh *Oracle*. Ini memungkinkan pengguna untuk menjalankan beberapa sistem operasi di dalam satu mesin fisik tanpa memerlukan penginstalan ganda atau partisi yang rumit. Dengan menggunakan konsep virtualisasi,

VirtualBox memungkinkan pengguna untuk membuat mesin virtual yang berfungsi sepenuhnya dan mandiri di dalam sistem operasi utama mereka.

VirtualBox mendukung berbagai sistem operasi tamu, termasuk Windows, Linux, macOS, dan banyak lagi. Ini memungkinkan pengguna untuk menguji perangkat lunak, mengembangkan aplikasi lintas platform, dan melakukan pengujian sistem tanpa mempengaruhi lingkungan produksi. Fitur utama VirtualBox termasuk *snapshot*, yang memungkinkan pengguna untuk membuat salinan titik pemulihan mesin virtual sehingga mereka dapat dengan mudah mengembalikan mesin ke keadaan sebelumnya. Selain itu, VirtualBox juga menyediakan akses ke port USB, penggunaan folder bersama untuk berbagi file antara mesin fisik dan virtual, dan pengaturan jaringan yang fleksibel untuk menghubungkan mesin virtual dengan jaringan fisik (Manoppo et al., 2020).

VirtualBox juga mendukung penggunaan ekstensi untuk meningkatkan fungsionalitasnya. Ekstensi ini termasuk dukungan USB 2.0 dan 3.0 yang ditingkatkan, integrasi penuh dengan desktop host, dan enkripsi mesin virtual.

Meskipun VirtualBox adalah solusi virtualisasi yang kuat dan gratis, ada juga versi VirtualBox yang lebih canggih dengan fitur tambahan yang disebut "*VirtualBox Extension Pack*". Ini menyediakan dukungan tambahan, seperti Virtual USB 2.0/3.0, dukungan perangkat nirkabel, dan penggunaan *Remote Desktop Protocol* (RDP) untuk mengakses mesin virtual dari jarak jauh. Secara keseluruhan, VirtualBox adalah alat yang sangat berguna bagi pengguna yang ingin menjalankan dan mengelola mesin virtual dengan mudah dan efisien di dalam lingkungan komputasi mereka (Wahidin et al., 2022).

2.3.2.2 Linux Ubuntu

Linux Ubuntu adalah salah satu distribusi Linux yang populer dan berbasis Debian. Ubuntu dikembangkan oleh perusahaan Canonical Ltd. dan merupakan sistem operasi sumber terbuka (*open-source*) yang dirancang untuk keperluan umum dan dapat digunakan di berbagai perangkat, termasuk komputer desktop, laptop, server, dan perangkat *Internet of Things* (IoT) (Manoppo et al., 2020). Berikut adalah beberapa ciri khas dari Ubuntu:

1. Kesederhanaan dan Ketersediaan

   Ubuntu menekankan pada kesederhanaan penggunaan dan pengalaman pengguna yang intuitif. Distribusi ini menyediakan antarmuka pengguna yang ramah pengguna, serta menyediakan aplikasi dan alat yang mudah diakses.

2. Model Rilis Berkala

   Ubuntu memiliki siklus rilis reguler dengan versi baru yang dirilis setiap enam bulan sekali. Setiap dua tahun, ada juga versi Long-Term Support (LTS) yang mendapatkan dukungan jangka panjang dan pembaruan keamanan selama lima tahun.

3. Lingkungan Desktop

   Ubuntu secara default menggunakan lingkungan desktop GNOME, yang memberikan tampilan dan pengalaman pengguna modern. Namun, ada juga varian Ubuntu yang menggunakan lingkungan desktop lain, seperti KDE Plasma (Kubuntu) atau Xfce (Xubuntu).

4. Aplikasi Bawaan dan Repositori

Ubuntu menyertakan berbagai aplikasi bawaan seperti *web browser*, pemutar musik, aplikasi perkantoran, pemutar video, dan banyak lagi. Selain itu, Ubuntu memiliki repositori perangkat lunak yang luas yang memungkinkan pengguna menginstal dan mengupdate ribuan aplikasi dan paket perangkat lunak secara mudah.

5. Komunitas yang Kuat

   Ubuntu memiliki komunitas pengguna yang besar dan aktif di seluruh dunia. Komunitas ini menyediakan dukungan, forum diskusi, tutorial, dan berbagai sumber daya lainnya untuk membantu pengguna Ubuntu.

6. Fokus pada Keamanan

   Ubuntu menempatkan penekanan kuat pada keamanan. Sistem operasi ini dilengkapi dengan alat keamanan bawaan seperti firewall, enkripsi disk, dan pembaruan otomatis yang membantu menjaga keamanan sistem.

Ubuntu telah mendapatkan popularitas karena stabilitas, kemudahan penggunaan, dan komitmen pada filosofi perangkat lunak sumber terbuka. Sebagai distribusi Linux yang populer, Ubuntu digunakan oleh individu, organisasi, dan lembaga pendidikan di seluruh dunia.

2.3.2.3 *Windows* 7

Windows 7 adalah sistem operasi yang dikembangkan oleh Microsoft. Dirilis pada tahun 2009, *Windows* 7 menawarkan antarmuka pengguna yang intuitif dan stabil. Fitur-fitur terkenal termasuk Start Menu yang ditingkatkan, taskbar yang dioptimalkan, dan kemampuan multitasking yang baik. *Windows* 7 juga menyediakan kompatibilitas yang baik dengan perangkat keras dan perangkat lunak

yang lebih lama. Selain itu, sistem operasi ini dilengkapi dengan keamanan yang ditingkatkan, termasuk Windows Defender dan Windows Firewall. Meskipun Windows 7 menjadi populer, Microsoft menghentikan dukungan resminya pada Januari 2020, sehingga disarankan untuk memperbarui ke versi Windows yang lebih baru untuk menjaga keamanan dan kinerja yang optima (Ilhamdi & Kunang, 2021).

Pada penelitian cuckoo sanbox menyarankan menggunakan sistem operasi windows 7 selain dapat menghemat ruang memori dan mendapatkan mengamatan yang lebih banyak.

2.3.2.4 *Cuckoo Sandbox*

Cuckoo Sandbox adalah platform analisis *malware* yang berbasis pada teknologi machine learning. Platform ini dirancang untuk mendeteksi, menganalisis, dan memahami perilaku *malware* secara otomatis. Dalam konteks *machine learning*, *Cuckoo Sandbox* menggunakan pendekatan yang disebut supervised learning (pembelajaran terawasi).

Pertama, *Cuckoo Sandbox* dikonfigurasi dengan sejumlah fitur dan parameter yang digunakan untuk mengumpulkan data perilaku dari sampel malware yang dijalankan dalam lingkungan yang terisolasi. Fitur-fitur ini dapat mencakup kegiatan seperti pembukaan file, pengiriman data jaringan, atau perubahan konfigurasi sistem. Data perilaku ini kemudian digunakan sebagai input untuk melatih model *machine learning* (Wahidin et al., 2022)

Dengan menggunakan teknik pembelajaran terawasi, *Cuckoo Sandbox* memanfaatkan dataset yang telah dilabeli dengan baik untuk melatih model dalam

mengenali pola dan karakteristik yang mencurigakan dari malware. Setelah dilatih, model dapat diterapkan untuk mengklasifikasikan sampel malware yang tidak diketahui berdasarkan perilaku mereka.

Keuntungan utama dari menggunakan *Cuckoo Sandbox* dengan *machine learning* adalah kemampuannya untuk mendeteksi varian baru dan menganalisis *malware* yang belum pernah ditemui sebelumnya. Dengan melihat pola dan perilaku yang tidak biasa, *Cuckoo Sandbox* dapat mengidentifikasi tindakan berbahaya yang dilakukan oleh *malware*.

Cuckoo Sandbox juga memberikan laporan yang terperinci tentang aktivitas *malware* yang dianalisis. Ini memungkinkan para peneliti keamanan untuk memahami secara mendalam bagaimana malware beroperasi dan berinteraksi dengan sistem. Informasi ini penting dalam pengembangan strategi keamanan yang efektif dan perlindungan yang lebih baik terhadap ancaman *malware*.

Secara keseluruhan, *Cuckoo Sandbox* dengan pendekatan *machine learning* merupakan alat yang efektif dalam analisis malware yang otomatis dan dapat membantu mengidentifikasi ancaman baru dengan cepat dan akurat.

2.3.2.5 *Volatility Framework*

Sebuah framework forensik memori sumber terbuka yang digunakan untuk menganalisis memori volatile (RAM) pada sistem komputer. Dalam konteks ini, Volatility Framework Python merujuk pada implementasi yang dibangun menggunakan bahasa pemrograman Python.

Volatility Framework Python memberikan antarmuka pemrograman yang kuat untuk mengakses dan menganalisis data memori. Ini memungkinkan pengguna

untuk mengembangkan skrip dan alat khusus yang sesuai dengan kebutuhan mereka dalam melakukan analisis forensik memori (Demertzis et al., 2019).

Dalam menggunakan Volatility Framework Python, pengguna dapat mengakses struktur data dan informasi penting dari memori sistem yang sedang berjalan. Ini termasuk proses, modul, koneksi jaringan, layanan sistem, peta memori, dan banyak lagi. Dengan akses langsung ke memori, analis forensik dapat mengidentifikasi malware, mencari tanda-tanda serangan, dan mendapatkan wawasan mendalam tentang aktivitas sistem (Manoppo et al., 2020)

Selain itu, Volatility Framework Python juga menyediakan berbagai utilitas dan fungsi bawaan untuk membantu proses analisis. Ini mencakup dukungan untuk memecahkan struktur data seperti TEB *(Thread Environment Block)* pada Windows, analisis registri, analisis tumpukan *(stack)*, pemulihan file dari memori, dan banyak lagi.

Volatility Framework Python adalah alat yang berguna bagi para profesional forensik dan keamanan yang ingin melakukan analisis mendalam pada memori sistem. Dengan fleksibilitas Python, mereka dapat mengembangkan dan mengotomatisasi proses analisis dengan lebih efisien.

2.4 Penelitian Terdahulu

1. Bagus Aji Saputro, Volume 2 No. 10, ISSN 2714-7975 tahun 2021 dengan judul “Analisis Malware Android Menggunakan Metode Reverse Engineering” menyimpulkan bahwa *smartphone* merupakan perangkat yang aktif menggunakan internet maka dari itu penyerangan sangat berpotensi tinggi. Penulis menggunkanan proses. Secara keseluruhan,

analisis *malware* dengan *reverse engineering* adalah metode penting dalam memahami dan melawan serangan malware. Dengan mempelajari kode dan perilaku *malware*, analis dapat mengidentifikasi sasaran dan kerentanan yang digunakan oleh penyerang, dan mengembangkan solusi yang lebih efektif untuk melindungi sistem dan data dari ancaman tersebut.

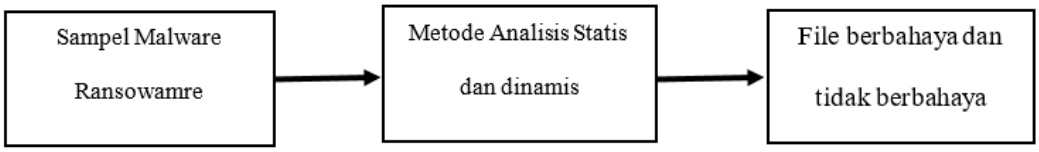
2. Virgiawan A. Manopo,Volume 9 No. 3, ISSN 2301-8402 tahun 2020 dengan judul "Analisa Malware Menggunakan Metode *Dynamic Analysis* Pada Jaringan Universitas Sam Ratulangi". Melakukan penelitian malware *Ransomware* denan metode analisis dinamis dengan tujuan tujuan adalah untuk menganalisa karakteristik malware yang ditemukan pada jaringan Universitas Sam Ratulangi. Adapun metode yang dipakai dalam penelitian ini adalah dengan *Dynamic Analysis* dan menggunakan *tool Cuckoo Sandbox*, sehingga tidak ada resiko untuk terinfeksi malware. Berdasarkan analisa yang dilakukan tentang karakteristik dari *malware*, dapat disimpulkan bahwa terdapat beberapa *signature, string,* dan perubahan pada *value registry*.
3. Arif Rachmat, Volume 2, No. 1 ISSN 2622-8254 tahun 2019 yang berjudul "Survei Penerapan Model Machine Learning Dalam Bidang Kemanan Informasi" Peneliti meguji efektivitas tujuh metode yang ada untuk analisa keamanan informasi. Pemanfaatan model machine learning dalam membangun aplikasi keamanan informasi telah menjadi keharusan untuk saat ini. Para peneliti terus mengem bangkan model dan algoritma serta melakukan optimalisasi dari sisi kemampuan analisis terhadap metode-

metode terbaru serangan keamanan informasi dan pelanggaran terhadap data privasi pengguna.

4. Demertzis K, Volume 3 No. 6 DOI 10:3390 Tahun 2019 yang berjudul *"The Next generations cognitive security operations center:Adaptive analytic Lambda architecture for efficient defense against adversarial attacks*. Melakukan peneltian yang berguana untuk membantu organisasi dalam mendeteksi serangan keamanan yang lebih kompleks dan terkini, mengurangi waktu respons terhadap insiden keamanan, serta meningkatkan efisiensi dan akurasi dalam analisis dan mitigasi ancaman. Dengan memadukan kecerdasan buatan dan kemampuan manusia, NGCC SOC dapat menjadi salah satu alat yang efektif dalam melindungi organisasi dari ancaman keamanan yang semakin canggih dan kompleks.
5. Alornyo S, DOI: 10.1109/ICASTECH.2018.8507063 tahun 2018 dengan judul "*Encrypted Traffic Analytic using Identity Based Encryption with Equality Test for Cloud Computing*" melakukan pengujian terhadap layanan cloud. Enkripsi Berbasis Identitas dengan Uji Kesetaraan adalah pendekatan untuk menganalisis lalu lintas terenkripsi dalam komputasi awan. Teknik ini melibatkan penggunaan enkripsi berbasis identitas untuk melindungi data yang dikirim melalui cloud. Uji kesetaraan digunakan untuk memverifikasi kunci enkripsi tanpa harus membuka pesan terenkripsi. Dengan menggunakan pendekatan ini, lalu lintas terenkripsi dapat dianalisis tanpa mengorbankan keamanan dan privasi. Ini memungkinkan organisasi

untuk memanfaatkan keuntungan komputasi awan sambil menjaga keamanan data mereka

2.5 Kerangka Pemikiran



Gambar 2. 4 Kerangka Pemikiran Penelitian Analisa *Ransomware*
(Sumber Penelitian : 2023)

Input : Pada Penelitian ini penulis membuat kerangka pemikiran secara umum untuk memudahkan pemetaan dan langkah penelitian. Adapaun input dari penelitian ini adalah menganalisa *malware* seperti pada gambar 2.3

Proses : menganalisa *malware ransomware* dengan metode statis dan dinamis, terakhir

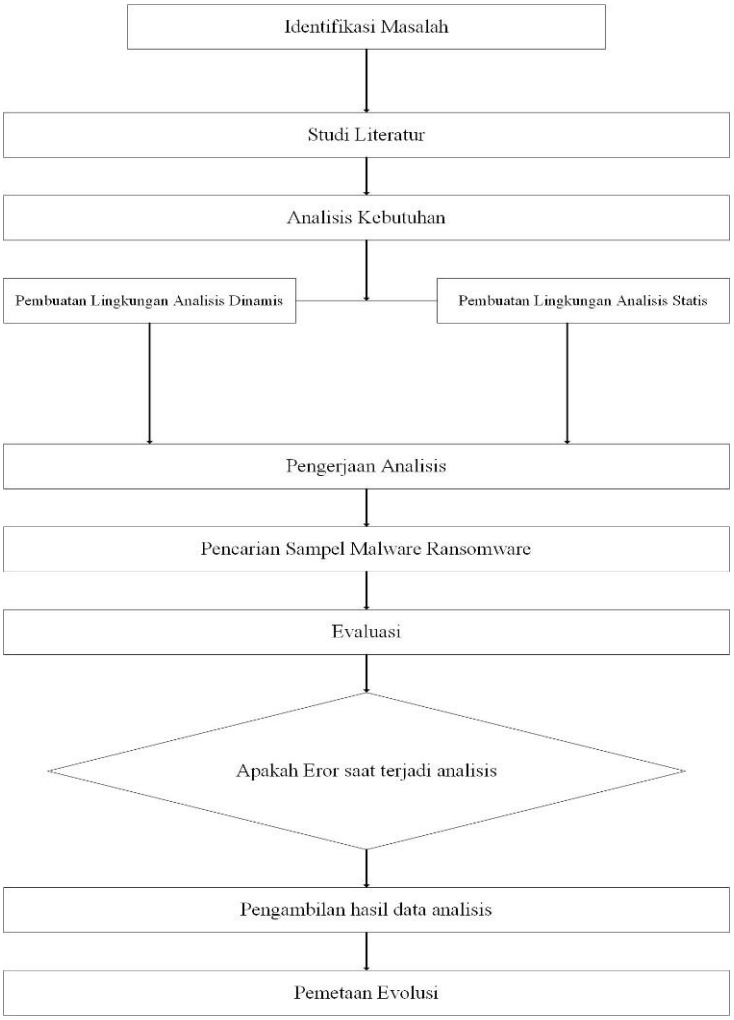
Output : penelitian ini penulis dapat menyimpulkan file yang berbahaya atau tidak berbahaya berdasarkan pengamatan pada tahapan proses.

BAB III

METODE PENELITIAN

3.1 Desain Penelitian

Penulis merancang sebuah desain sistematis analisis *malware ransomware* dengan membandingkan hasil dari kedua metode yang disimpulkan dalam perbandingan tabel dengan analisis kualitatif (Fadli, 2021) Adapun skema atau desain penelitian sebagai berikut:



Gambar 3. 1 Alur Penelitian Analisis *Malware*
(Sumber Penelitian: 2023)

1. Pada tahapan ketiga peneliti melakukan studi literatur dari berbagai sumber dan jurnal untuk mendapatkan metode yang akan diterapkan.
2. Pada tahapan keempat peneliti menggunakan dua metode analisis *malware ransomware* yaitu metode statis dan dinamis. Kedua metode ini diterapkan pada jenis sistem operasi yang berbeda, serta tools yang akan digunakan untuk mendukung proses kedua analisis tersebut.
3. Pada tahapan kelima peneliti mengambil beberapa sampel ransomware yang akan digunakan untuk pengujian dari berbagai sumber.
4. Setelah mendapatkan beberapa sampel jenis *malware* pada tahapan keenam peneliti mengevaluasi terlebih dahulu sampel yang akan digunakan dalam *sanbox* buatan dan terpisah dari jaringan PT.NPCB untuk mengurangi resiko tersebarnya *malware ransomware* jika terjadi kesalahan.
5. Pada tahapan ketujuh peneliti mengambil hasil dari beberapa tahapan dan *tools* yang digunkan.
6. Pada proses tahapan kedelapan meneliti mengamati apakah ada kendala dari kedua analisis tersebut baik secara tools atau sampel yang digunakan.
7. Pada tahapan kesembilan peneliti melakukan peta evolusi perkembangan *malware* jenis *ransomware* dari tahun ke tahun.

3.2 Analisis Keamanan Jaringan yang Berjalan

PT. NPCB menggunakan komputer sebanyak 26 client dan satu server sebagai alat bantu operasional dan perangkat 4 printer *sharing* serta 2 mesin fotocopy untuk penunjang operasional. Implementasi jaringan menggunakan *full wired(ethernet wire)* sebagai media transmisi jaringan. Kapasitas *bandwidth* yang

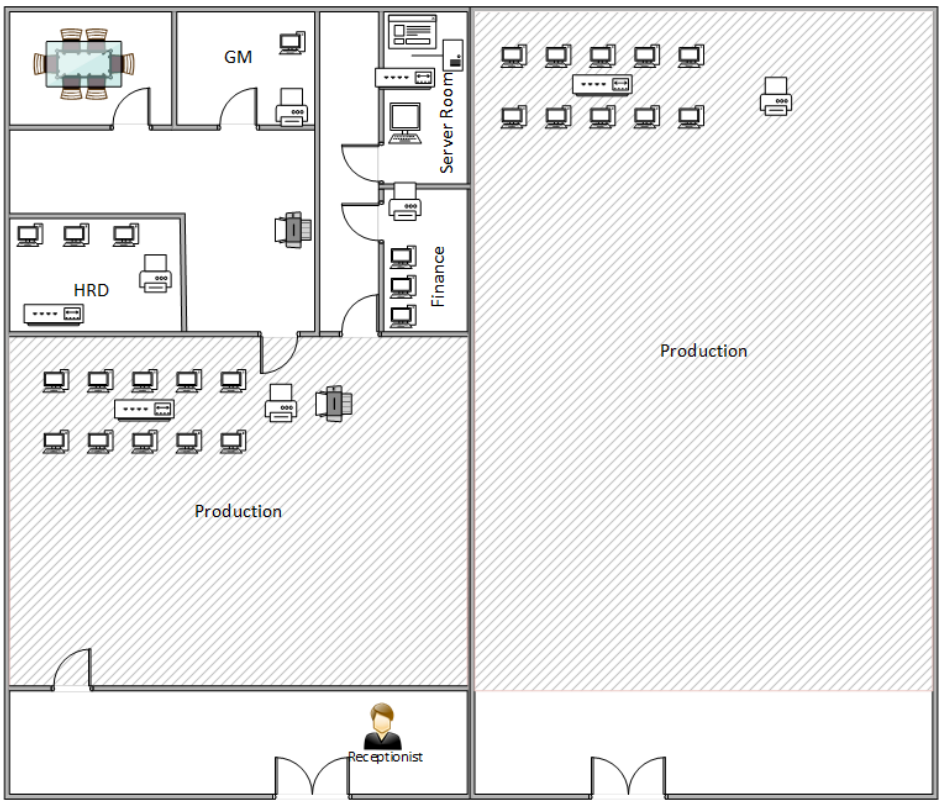
digunakan layanan dedicated 50 Mbps dengan layanan *provider* jasa Batam Bintan Telekomunikasi (BBT). Pada masing-masing client menggunakan windows 10 profesional dan server menggunakan *windows* server 2016. Adapun antivirus yang digunakan adalah AVG *bussiness class*. Berikut tabel analisa *hardware* pada jaringan dan sistem yang berjalan pada PT. NPCB:

Tabel 3. 1 Tabel perangkat jaringan PT. NPCB

Class	Spec	OS	Qty	Remarks
Server PC	Intel Xeon 4110 8C 2.1GHz, Storage 5 TB, RAM 2x8 GB	Windows Server 2016	1	Powered by AVG
Client PC	Lenovo Core i5 gen 10, Ram 8 GB, Storage 500 gb	Windows 10 Profesional	26	Powered by Windows firewall and AVG
Printer	Epson L6190	-	4	
Fotocopy	Fujixerox	-	1	
Router	Cisco	Cisco Router	1	
Hub/Switch	16 Port	Unmanaged Switch	4	
Firewall	Fortiget	FortiOS	1	

Pada topologi jaringan lama team IT PT.NPCB menggunakan layanan antivirus dan firewall function dari bawaan windows server dan firewall fortiget

sebaga pilar utama untuk keamanan jaringan. Selain itu untuk client menghindari penggunaan USB eksternal untuk memindahan data dan melakukan *blocking* dari *website-website* yang mengandung *malware.*



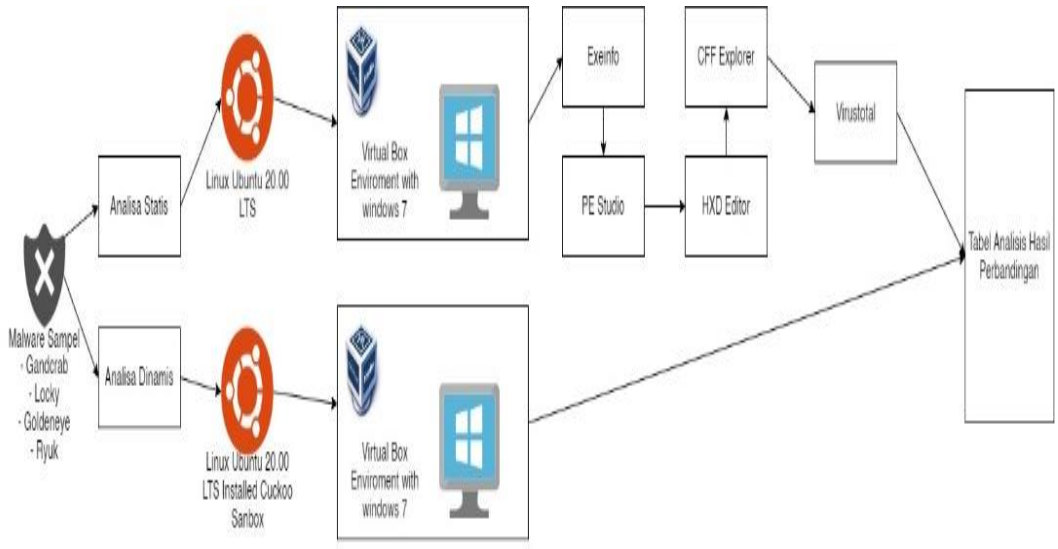
Gambar 3. 2 Topologi jaringan PT. NPCB
(Sumber Penelitian: 2023)

3.3 Kebutuhan Sistem Analisis Ransomware

Pada rancangan analisis kemanan jaringan baru di PT.NPCB team *IT* dan peneliti bekerja sama untuk mempelajari jenis-jenis *ransomware* khususnya jenis *Gandcrab*, *Petya* didapat dari *Github*.

Dengan membuat *enviroment* terpisah dengan bantuan linux dan virtualbox agar selamasa proses analisa sampel *malware* yang akan diperiksa tidak menyebar

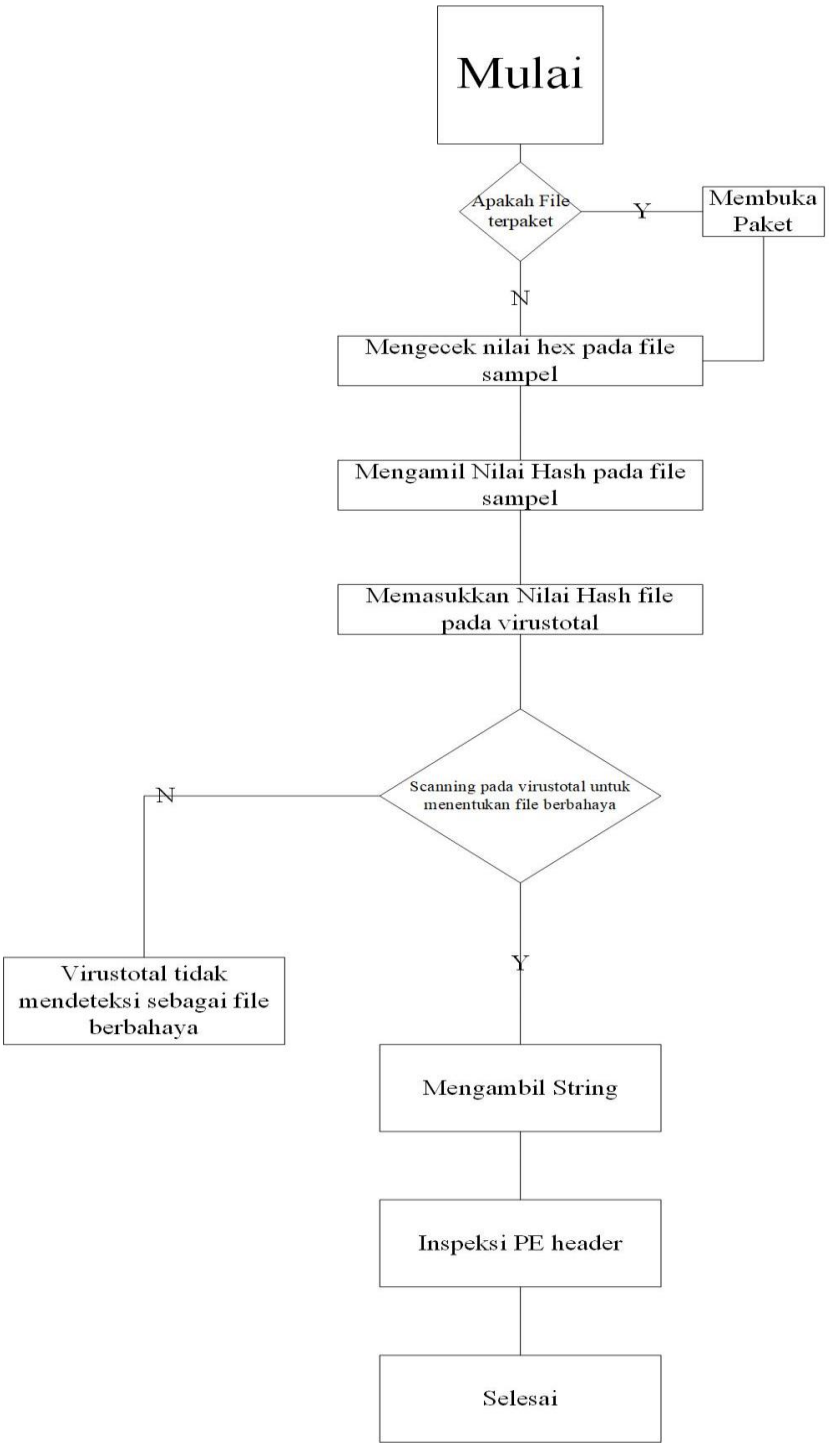
ke lingkungan jaringan PT.NPCB. Berikut topologi dari rancangan analisis keamanan yang akan diterapkan oleh peneliti:



Gambar 3. 3 Rancangan Kebutuhan Sistem Analisa Malware Ransomware (Sumber Penelitian: 2023)

3.3.1 Rancangan Penelitian Analisis Statis

Berikut tahapan pada alur proses analisis statis:



Gambar 3. 4 Alur Penelitian *Malware* Statis
(Sumber Penelitian:2023)

3.3.2 Installasi Sistem

Peneliti menggunakan sistem operasi *windows* 7 yang sudah terisolasi dengan bantuan virtualbox agar saat melakukan analisa tidak menyebabkan *eror* ke jaringan komputer yang sedang berjalan. Beberapa *tools* analisis statis ini berjalan di sistem operasi *windows* 7 dan melakukan installasi seperti *software* pada umumnya. Adapun *tools* dan sumber yang digunakan sebagai berikut:

Tabel 3. 2 Sumber aplikasi

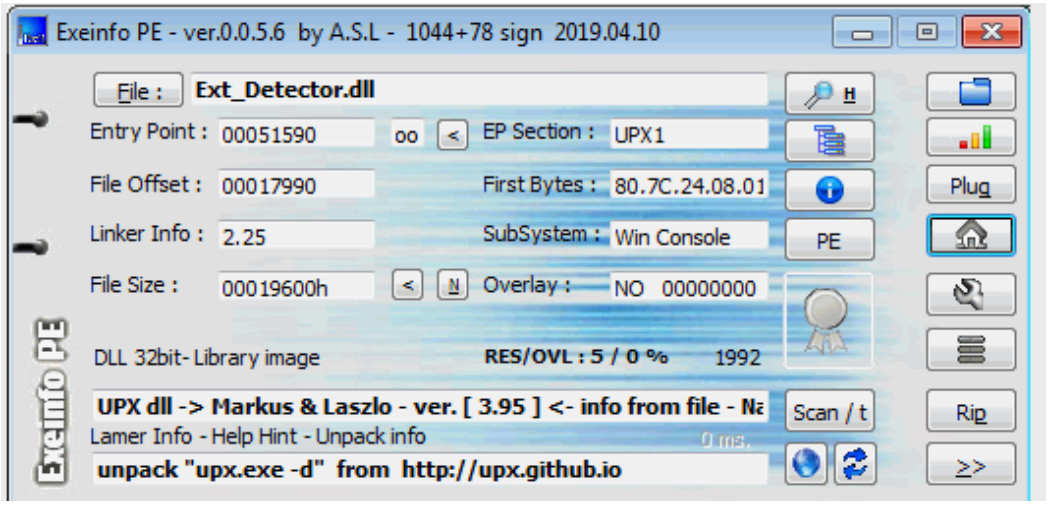
Aplikasi	Sumber	Operasi Sistem
PE Studio	https://www.winitor.com/download	Windows 7
CFF Explorer	https://github.com/cybertechniques/site/blob/master/analysis_tools/cff-explorer/index.md	Windows 7
Hxd Editor	https://mh-nexus.de/en/hxd/	Windows 7
Virustotal	https://www.virustotal.com/	Windows 7

3.3.3 Analisis jenis file terdapat paket

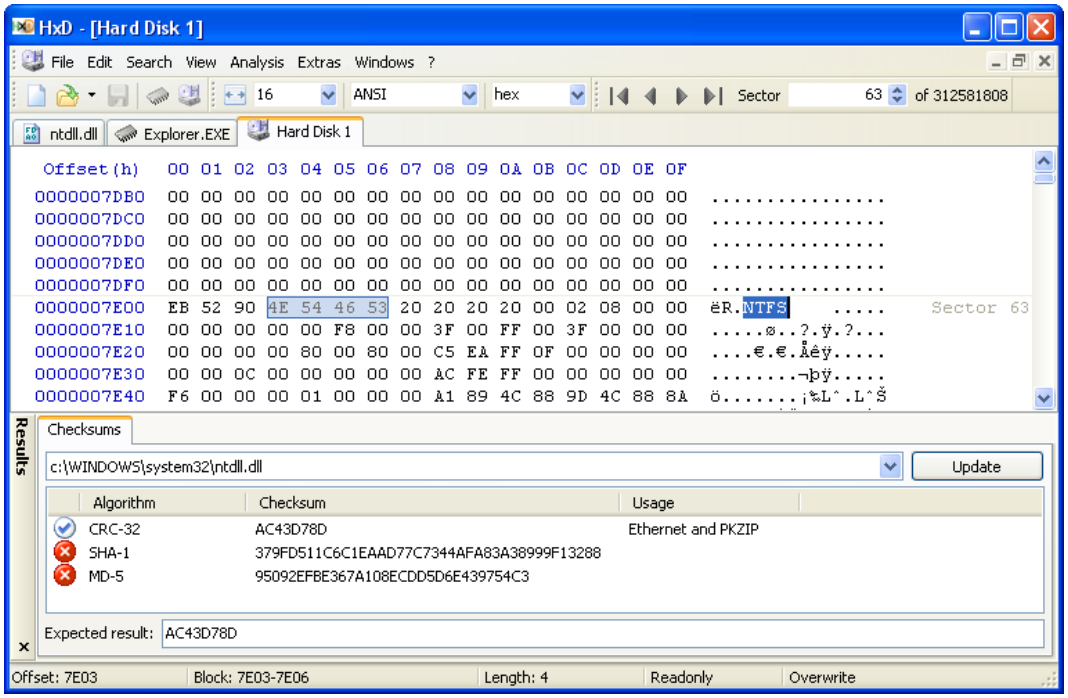
Biasanya, *ransomware* didistribusikan dalam bentuk paket. Paket ini memiliki kemampuan untuk menghapus *ransomware* dari file asli, membuatnya tampak seperti perangkat lunak yang aman. Jika *ransomware* sudah dipaketkan, file yang bersangkutan tidak dapat diperiksa dengan cermat, dan jika *ransomware*

diperiksa dalam bentuk paket, string hash dan analisis hash lainnya tampak tidak normal dan tidak dapat didekripsi. Ketika *ransomware* dalam bentuk paket file diaktifkan, file-file tersebut akan didekompresi dan file yang ditargetkan akan diaktifkan.

Identifikasi jenis file ini diperlukan untuk memahami jenis *ransomware* yang aktif, serta sistem operasi (*Windows*, Linux, dll), dan arsitektur (32-bit atau 64-bit). Jika *ransomware* menggunakan format file *portable executable* (PE), ia memiliki informasi tentang format file yang dapat dibuka oleh *Windows* (.exe,.dll,.sys,.drv, dll). Dari informasi ini, jelas bahwa ransomware yang dimaksud merusak sistem *Windows*.



Gambar 3. 5 Tampilan ExeInfo PE
(Sumber Penelitian:2023)



Gambar 3. 6 Tampilan Hxd
(Sumber Penelitian: 2023)

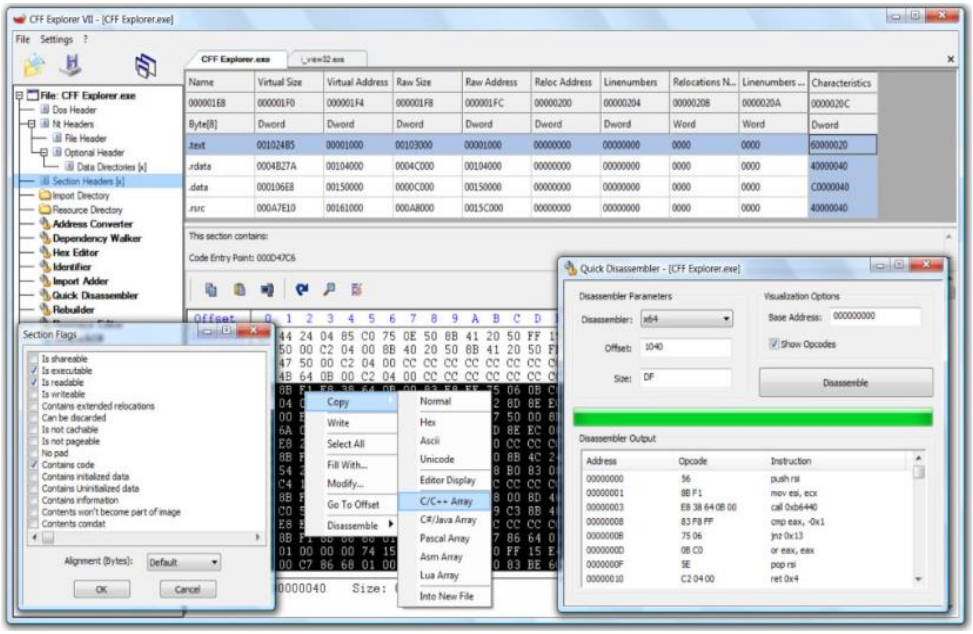
Pada gambar 3.6, ditampilkan metode manual untuk memahami jenis file. Ada banyak metode yang dapat digunakan untuk menentukan jenis file, termasuk CFFexplorer, PE32, dan Python. Dari hasil alat manual HxD, contoh cara memahami dasar-dasar jenis file adalah dengan melihat nilai awal 2 bit dari kode heksadesimal 4D 5A; jika ditulis dalam ASCII, ini akan menghasilkan pembuatan MZ, dan dari data yang diperoleh, 2 bit itu sendiri dapat diambil. Metode manual memiliki kekurangan, tetapi harus digunakan untuk mendapatkan lebih banyak pengetahuan tentang bagaimana setiap file memiliki pola bit yang unik sehingga komputer dapat mengenali jenis file untuk meluncurkan file yang perlu dieksekusi.

3.3.4 Sidik Jari *Ransomware*

Virus yang disebut Sidik Jari Sidik Jari menghasilkan nomor hash kriptografi untuk membuat nomor biner berdasarkan isi file. Nilai hash yang valid adalah MD5, SHA1, atau SHA256. Tujuan dari nilai hash ketika menganalisis ransomware adalah untuk:

1. Mengenali *ransomware*, bahkan ketika ransomware memiliki nama yang berbeda ketika file terenkripsi digunakan.
2. Jika nilai hashnya sama, maka *ransomware* akan tetap dikenali sebagai *ransomware* yang sama..
3. Analisis yang realistis adalah bahwa *ransomware* akan meningkatkan permintaan uang dan mulai menyebar. *Ransomware* yang sedang aktif akan terus memiliki nilai hash yang sama.
4. Nilai hash dapat membantu dalam identifikasi ransomware dan file.

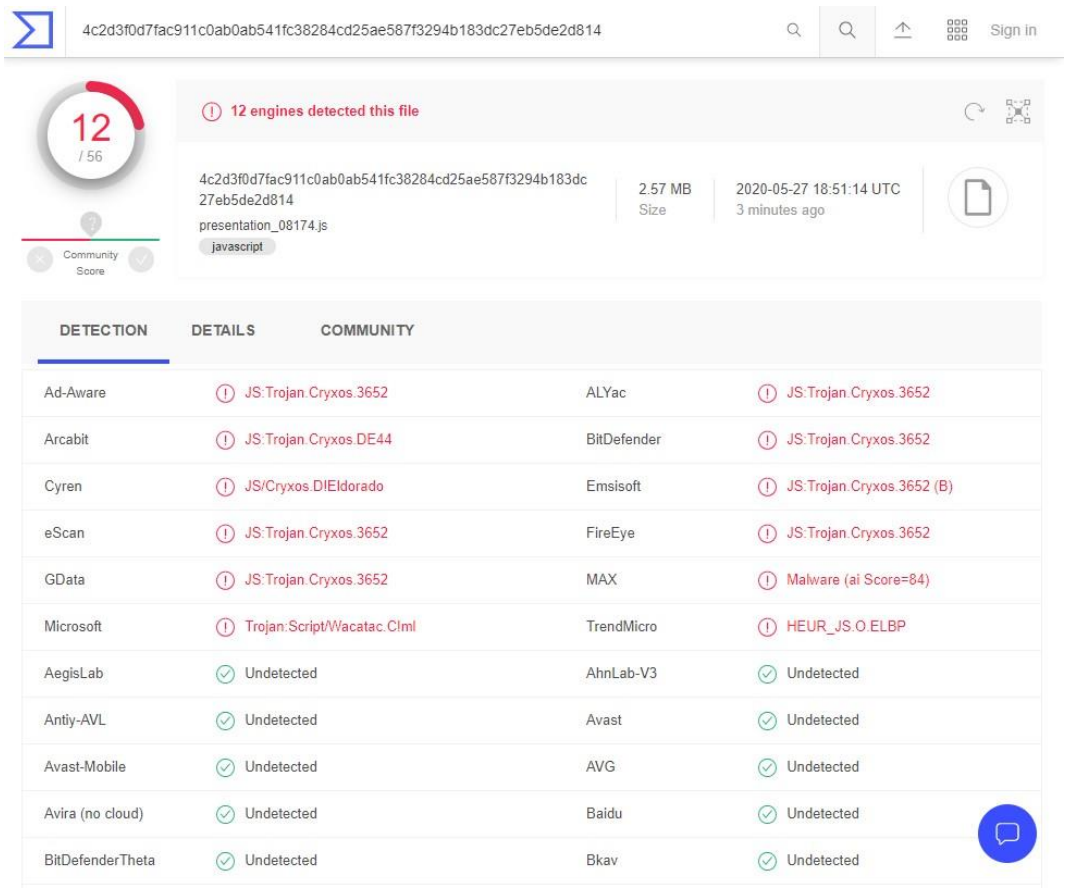
Nilai hash dapat dibuat menggunakan CFFexplorer atau PeStudio, dan kemudian akan diunggah ke situs *web* VirusTotal untuk mengumpulkan informasi yang *komprehensif*.



Gambar 3. 7 Tampilan CFF Explorer
(Sumber Penelitian:2023)

3.3.5 Pemindaan Informasi Sampel *Ransomware*

Pemindaian dapat mengindikasikan apakah sebuah file mengandung kode biner yang dapat merusak sistem. Hasil dari pengujian berbagai program antivirus akan membantu dalam analisis yang lebih menyeluruh karena setiap antivirus memiliki ambang batas pemindaian dan tingkat deteksi ransomware yang berbeda.



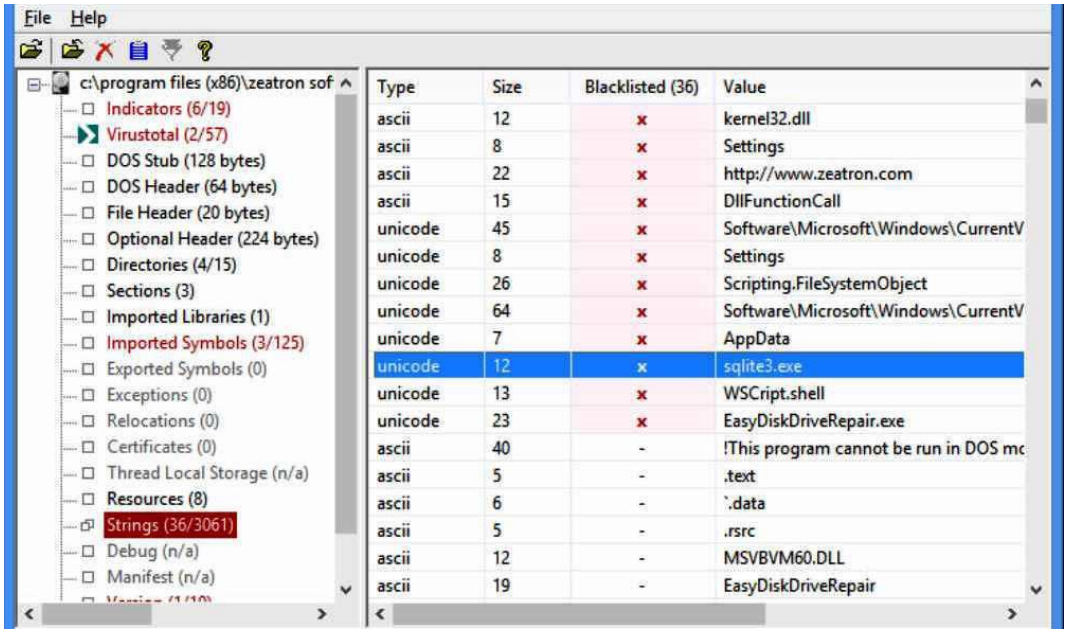
Gambar 3. 8 Tampilan Proses Virustotal
(Sumber Penelitian:2023)

Hasil dari pengujian yang dilakukan dengan VirusTotal yang dilakukan di situs VirusTotal. Dengan menggunakan nilai hash yang didapatkan dari data yang bersangkutan, maka dapat diambil sebuah kesimpulan. Jika sebuah file dikonfirmasi sebagai file yang valid berisi *advice*, maka analisis akan dimulai, namun jika file yang diperiksa tidak memberikan hasil positif yang mengindikasikan bahwa file tersebut berisi *advice*, maka tidak perlu dilakukan analisis lebih lanjut.

3.3.6 Mengambil Nilai *String*

String file terdiri dari karakter ASCII dan *Unicode*. Manipulasi string dapat memberikan informasi tentang bagaimana sebuah perangkat lunak beroperasi. Misalnya, jika *ransomware* memiliki kemampuan untuk membuat file, nama file tersebut akan ditampilkan sebagai string; jika *ransomware* memiliki nama domain yang dikendalikan oleh penyerang, nama domain tersebut akan ditampilkan sebagai string; dan informasi lain yang dapat mengungkapkan kemampuan *malware* juga akan ditampilkan sebagai string.

.



Gambar 3. 9 Tampilan PE Studio
(Sumber Penelitian:2023)

String dapat mengungkapkan cara kerja *ransomware* selama infeksi, tetapi untuk memastikannya, proses analisis yang terperinci harus dilakukan untuk mengidentifikasi cara kerja *ransomware* secara akurat. Tidak semua string yang

diperluas memiliki nilai numerik yang berguna untuk analisis; contoh dari string tersebut termasuk nama file, URL, alamat IP, dan Kunci Registri.

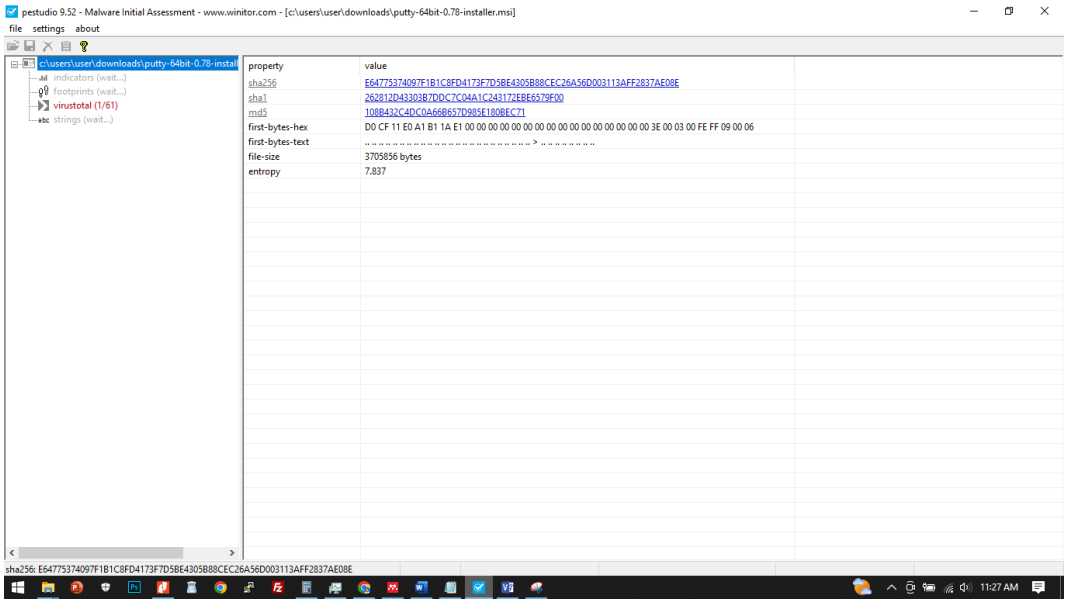
3.3.7 Inspeksi PE *Header*

PE *header* adalah komponen penting dalam melakukan analisis statistik karena mengandung banyak informasi yang berguna. Sebagai contoh, header PE berisi rincian tentang bagaimana sistem operasi meluncurkan file yang dapat dieksekusi, bagaimana ransomware berinteraksi dengan sistem operasi, dan kondisi di mana file yang dapat dieksekusi harus disimpan di dalam memori dan dapat digunakan untuk mengidentifikasi file-file yang akan dieksekusi. Selain itu, header PE berisi informasi tentang perpustakaan yang digunakan oleh ransomware.

Tabel 3.3 Tabel Penjelasan dari PE header

Variabel	Penjelasan
MZ Header/DOS *Header*	Mendefenisikan file sebagai executable binary
DOS Stub *(Program Cannot be run in DOS Mode)*	Untuk menampilkan pesan jika dijalankan dalam DOS (untuk pengecekan kompabilitas)
PE *File Header* (*signature*)	Mendefenisikan executable sebagai PE
Image Optional *Header*	Menyimpan informasi tentang executable seperti subsystem dan entry point
Section Tabel	Intruksi bagaimana memuat executable kedalam memori
Section	Komponen dari code executable dan data yang digunakan oleh executable

diatas menjelaskan bagian-bagian dari PE *header* dimana setiap bagian *header* menjelaskan informasi yang berbeda dan pada gambar dijelaskan tampilan file *header* seperti yang dijelaskan dalam file *header* adalah tempat informasi yang mendefinisikan bahwa file ini adalah file *executable*, serta informasi kapan file pertama kali di-compile.



Gambar 3. 10 Tampilan PE Studio
(Sumber Penelitian:2023)

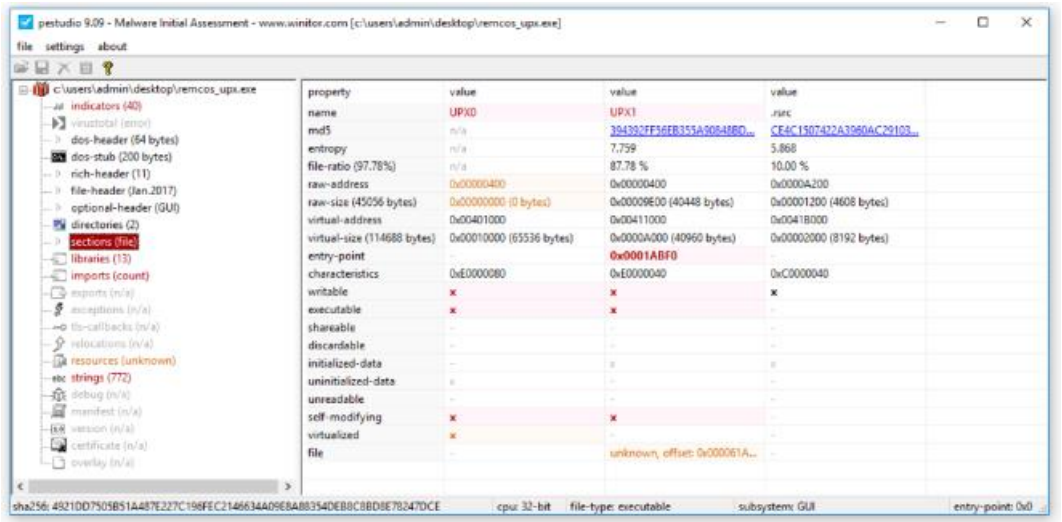
Dapat dilihat dalam tabel diatas penjelasan bagian bagian PE *header* dan pada bagian section disebutkan tentang data yang akan di jelaskan pada tabel di bawah:

Tabel 3. 4 Daftar Header dan Fungsi

Nama Header	Fungsi
.code/.text	Kode executable
.data	Menyimpan data(R/W)
.rdata	Menyimpan data (read only)

.idata	Menyimpan data improt
.edata	Menyimpan data export
.rsrc	Menyimpan resources data (string dan icon)

Untuk dimengerti PE atau *Portabel Executable* bukan berarti hanya dimiliki oleh *ransomware* namun semua file memiliki PE, dan apa yang membedakan dari tabel.

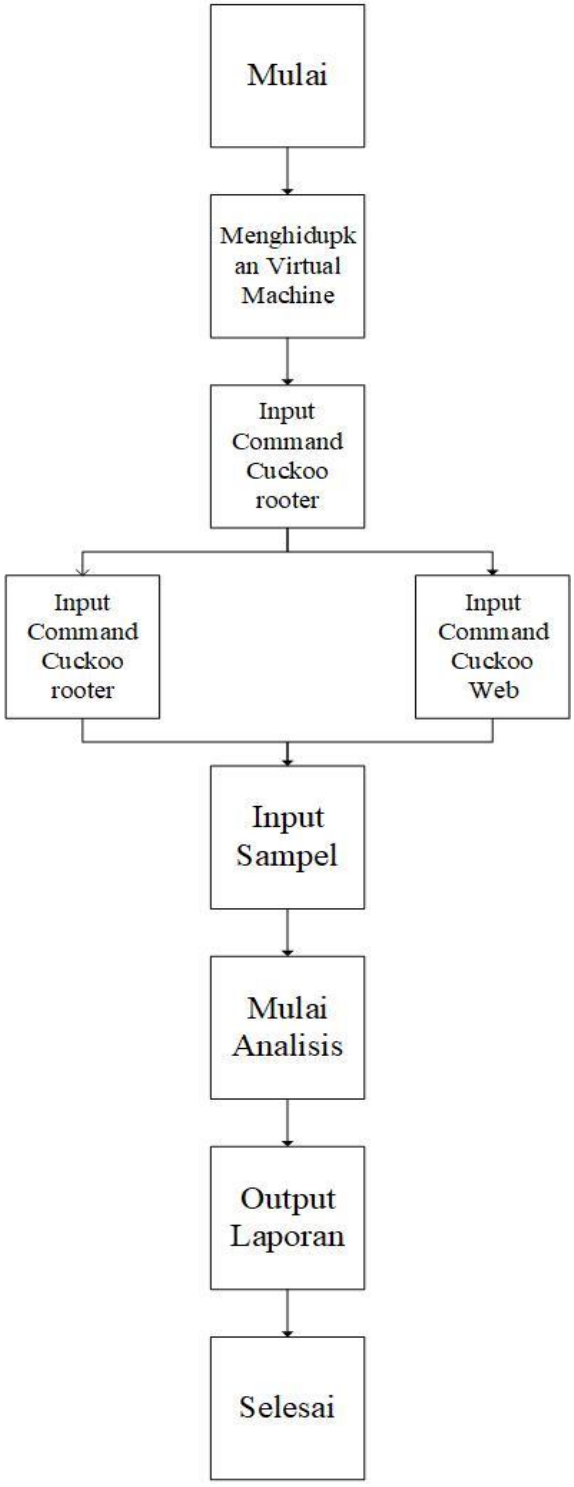


Gambar 3. 11 Tampilan Section pada PE Studio
(Sumber Penelitian:2023)

Gambar 3.8 merupakan bagian dari s*ection* yang menampilkan apa yang dijelaskan pada tabel 3.1 dan banyak informasi lainya seperti *entry-point*, *writeable*, *executable*, *virtual-size*, dan *raw-size*. Namun pada inspeksi PE *header* dapat ditelusuri lagi lebih dalam dengan melihat informasi *import*, *library* dan *resource* yang akan dijelaskan lebih detail pada BAB IV.

3.3.8 Rancangan Penelitian Analisis Dinamis

Berikut alur penelitian dinamis:



Gambar 3. 12 Alur Penelitian *Malware* Dinamis
(Sumber Penelitian:2023)

3.4 Installasi Sistem

Berikut daftar kebutuhan *hardware* dan *software* yang dibutuhkan penulis untuk analisa dinamis:

Tabel 3. 5 Kebutuhan Perangkat Keras dan Lunak Analisis Dinamis

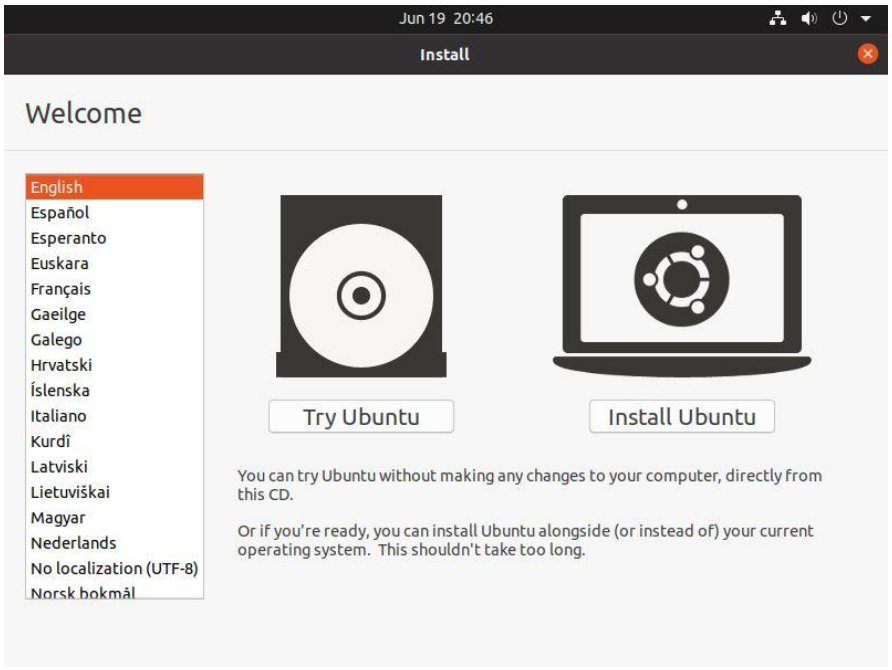
Kategori	Spesifikasi	Keterangan
Hardware	CPU AMD Ryzen 3 2200G, Ram 16GB,	CPU
Hardware	Monitor Dell 24 Inch	Monitor
Software	Linux Ubuntu 18.04 LTS	Operasi Sistem
Software	Virtualbox 7.02	App
Software	Windows 7 x64 bit	Operasi Sistem
Software	Yara-python	Library/PIP
Software	Distorm	Library/PIP
Software	Cuckoo	Library/PIP
Software	Pydeep	Library/PIP
Software	Ujson	Library/PIP
Software	tcpdump	Library/PIP

Pada proses penelitian analisis *malware* metode dinamis menggunakan *cuckoo sanbox* yang ditanamkan pada *Linux Ubuntu* berikut proses installasi sistem tersebut:

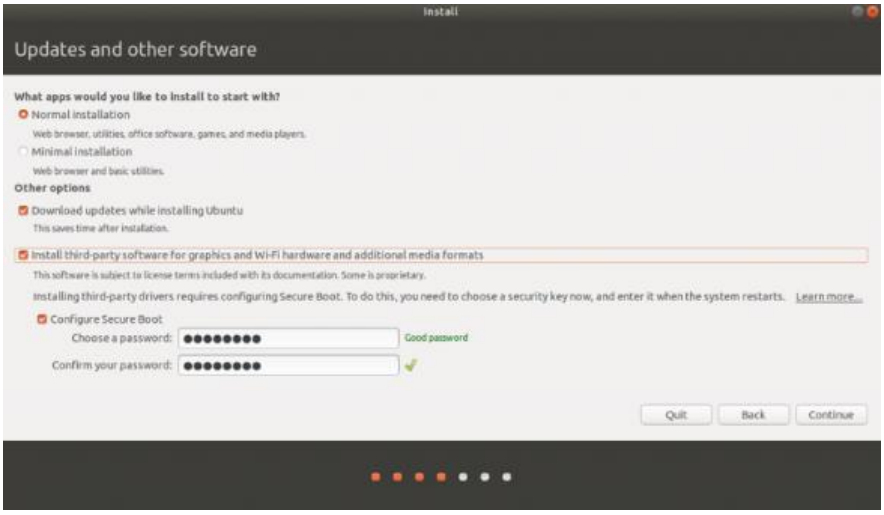
1. Download *Linux Ubuntu* pada proses ini penulis menggunakan versi 18.04 LTS yang mendukung penggunaan python versi 2.

Gambar 3. 13 Download Iso Image Ubuntu 18.04 LTS(Focal Fossa)
(Sumber Penelitian:2023)

2. Installasi menggunakan bantuan aplikasi rufus yang sudah ditanam menggunakan *disk image linux ubuntu* 18.04 LTS.

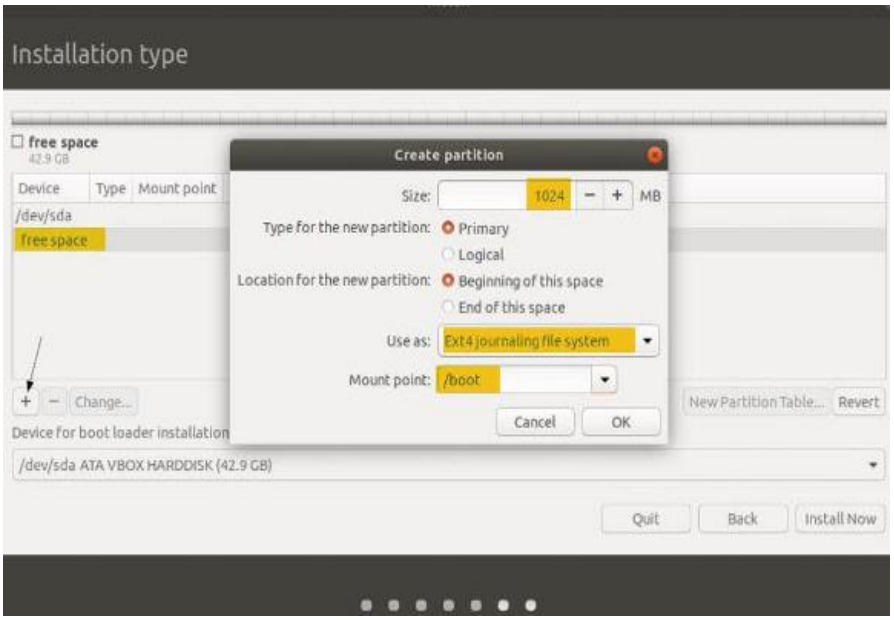


Gambar 3. 14 Proses Installasi Ubuntu
(Sumber Penelitian:2023)



Gambar 3. 15 Proses Installasi Ubuntu
(Sumber Penelitian:2023)

3. Melakukan pemilihan installasi *linux* dengan *other options* agar *linux* mendapatkan *update driver hardware*, dan *tools default* tambahan.



Gambar 3. 16 Proses Partisi Penyimpanan Linux
(Sumber Penelitian:2023)

4. Melakukan konfigurasi partisi penggunaan *disk* dengan *swap memory* 8192 mb, *home partition* 80 GB, *root partition* 50 GB.

5. Setelah itu menunggu proses installasi.

Gambar 3. 17 Instsallasi Linux
(Sumber Penelitian:2023)

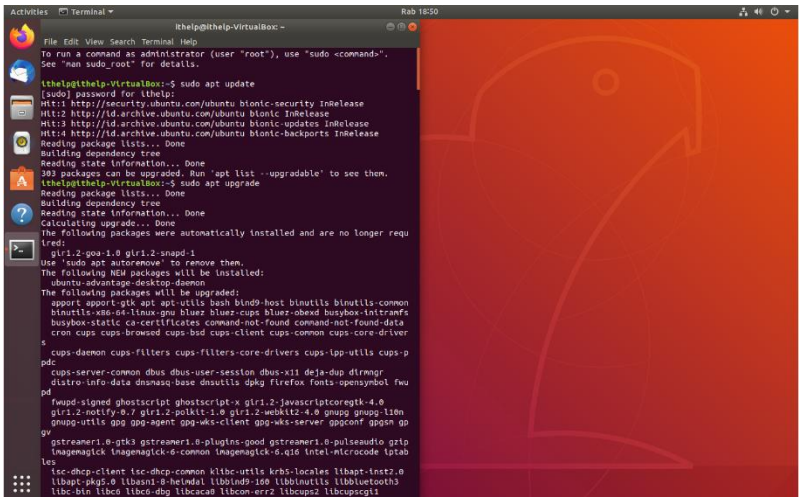
6. Setelah melakukan installasi *linux* operasi sistem lakukan *update* pada *repository linux* dengan *command* seperti berikut:

```
sudo apt upadate
sudo apt upgrade
```

7. *Ubuntu* 18.04 LTS didukung oleh *python* 2.7 dikarenakan *cuckoo* berjalan dengan *python* versi tersebut selanjutnya melakukan konfigurasi pada *user* "admin" dan menambahkan *library* pada *pip python* dengan *command* seperti berikut:

```
sudo apt-get update && sudo apt-get upgrade -y
sudo adduser admin
sudo adduser admin sudo
sudo apt-get install curl
curl https://bootstrap.pypa.io/pip/2.7/get-pip.py -o get-pip.py
sudo apt-get install python
```

```
sudo python get-pip.py
sudo apt-get install -y python-dev libffi-dev libssl-dev libfuzzy-dev
libtool flex autoconf libjansson-dev git
sudo apt-get install -y python-setuptools
sudo apt-get install -y libjpeg-dev zlib1g-dev swig
```



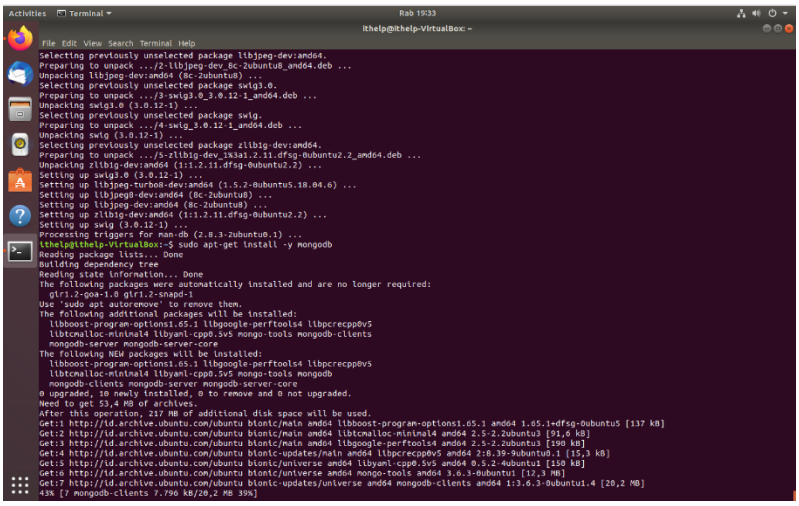
Gambar 3. 18 Proses Upgrade dan Update Reposiroty Linux
(Sumber Penelitian:2023)

8. Mengunduh *library cuckoo sandbox* dengan mengisikan *command* berikut pada terminal *Ubuntu*

```
sudo apt-get update
sudo apt-get upgrade
#Installasi Cuckoo Sanbox
sudo apt-get install -y python-dev libffi-dev libssl-dev libfuzzy-dev
libtool flex autoconf libjansson-dev git
#Installasi python tools
sudo apt-get install -y python-setuptools
#Installasi interface tools
sudo apt-get install -y libjpeg-dev zlib1g-dev swig
```

9. Installasi *MongoDB* dikarenakan *cuckoo sanbox* menggunakaan *database* versi *MongoDB* maka penulis melakukan installasi *MongoDB* pada terminal *linux* dengan perintah:

```
sudo apt-get install -y mongodb
sudo apt-get install -y postgresql libpq-dev
sudo apt-get install -y virtualbox
```



Gambar 3. 19 Installasi Mongo DB
(Sumber Penelitian:2023)

10. Installasi Virtualbox untuk menampung OS *windows* 7 dengan tujuan analisis *malware* tidak menyebar ke pengguna jaringan lainya.

```
sudo apt-get install -y virtualbox
cd Downloads/
~/Downloads
git clone https://github.com/volatilityfoundation/volatility.git
cd volatility
sudo python setup.py build
sudo python setup.py install
cd ..
```

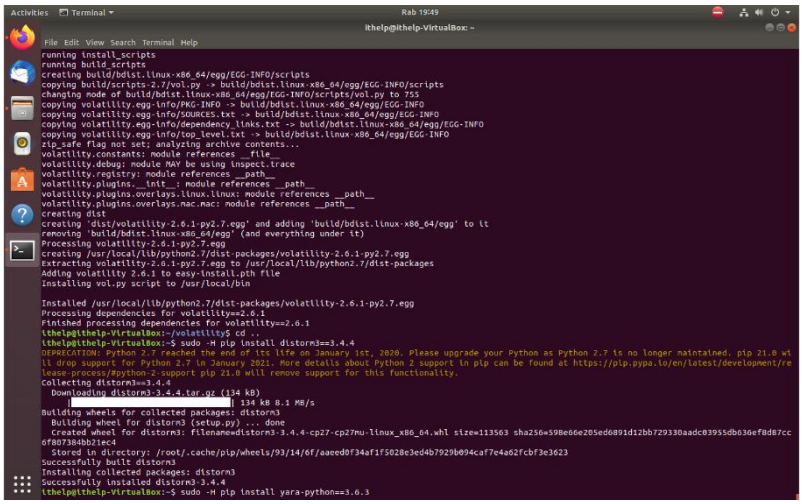
Gambar 3. 20 Download Virtualbox
(Sumber Penelitian:2023)

11. Kemudian melakukan installasi destorm3 yang bertujuan untuk melakukan *dekomposer* pada file dari teks ke bilangan biner dengan tujuan memudahkan analisis *malware*. Menggunakan distrom3 dikarenakan lebih unggul dibandingkan *tools opensource* lainnya untuk melakukan analisa tersebut.

```
sudo -H pip install distorm3==3.4.4
```

12. Melakukan installasi yara sebagai *tools* untuk membantu pengecekan sampel *malware*.

```
sudo -H pip install yara-python==3.6.3
```

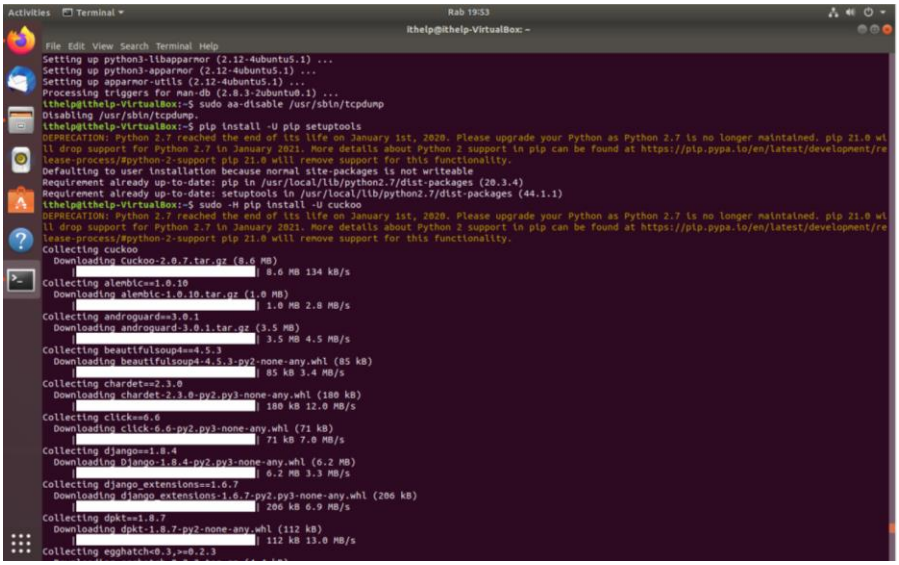


Gambar 3. 21 Installasi library python
(Sumber Penelitian:2023)

13. Selanjutnya melakukan installasi *tools SSDEEP* dan *pydeep*, *ssdeep*, *ujson*, *jupyter* dan *tcpdump*.

```
sudo apt-get install -y ssdeep
ssdeep -V
pip show pydeep
sudo -H pip install openpyxl
sudo -H pip install ujson
sudo -H pip install jupyter
sudo apt-get install tcpdump
sudo apt-get install libcap2-bin
```

sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
getcap /usr/sbin/tcpdump
sudo apt-get install -y apparmor-utils
sudo aa-disable /usr/sbin/tcpdump
pip install -U pip setuptools
sudo -H pip install -U cuckoo
cuckoo
sudo apt install -y net-tools
ifconfig
vboxmanage hostonlyif create
vboxmanage hostonlyif ipconfig vboxnet0 --ip 192.168.46.101 (IP VM yang digunakan)
ifconfig
sudo mkdir /opt/systemd/
sudo nano /opt/systemd/vboxhostonly
!/bin/bash hostonlyif create vboxmanage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1
cd /opt/systemd/
sudo chmod a+x vboxhostonly
sudo touch /etc/systemd/system/vboxhostonlynic.service
sudo nano /etc/systemd/system/vboxhostonlynic.service
#Konfigurasi Pada ethernet virtualbox
Description=Setup VirtualBox Hostonly Adapter
After=vboxdrv.service [Service] Type=oneshot
ExecStart=/opt/systemd/vboxhostonly [Install] WantedBy=multi-user.target
systemctl daemon-reload systemctl enable vboxhostonlynic.service



Gambar 3. 22 Proses Installasi Repositoy Cuckoo
(Sumber Penelitian:2023)

14. Selanjutnya melakukan installasi virtual *machine* dengan virtual box menggunakan operasi sistem *Windows* 7
15. Melakukan konfigurasi antaran virtual box dan *cuckoo sanbox webserver* dan IP *forwading*,

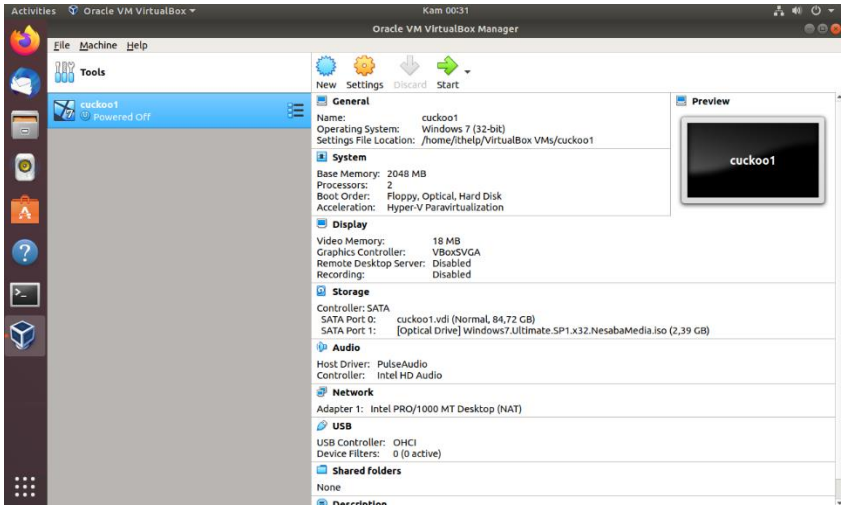
```
sudo apt-get install -y iptables-persistent
sudo iptables -A FORWARD -o eth0 -i vboxnet0 -s
192.168.56.0/24 -m conntrack --ctstate NEW -j ACCEPT

sudo iptables -A FORWARD -m conntrack --ctstate
ESTABLISHED,RELATED -j ACCEPT
sudo iptables -t nat -A POSTROUTING -o eth0 -j
MASQUERADE
sudo iptables -L
echo 1 | sudo tee -a /proc/sys/net/ipv4/ip_forward
sudo sysctl -w net.ipv4.ip_forward=1
sudo nano /etc/sysctl.conf
net.ipv4.ip_forward=1
sudo su –
iptables-save > /etc/iptables/rules.v4
~/.cuckoo/conf
cd .cuckoo/
cd ~/.cuckoo/conf
#melakukan konfigurasi pada cuckoo.conf
sudo nano cuckoo.conf
#edit pada gnome tersebut
machinery = virtualboxmemory_dump = yes
resultserver ip = 192.168.56.1
#Kemudian tekan crtl+x dan pilih yes untuk menyimpan
#Lakukan konfigurasi ke auxiliary.conf
sudo nano auxiliary.conf
enabled = yes
Kemudian tekan ctrl+x dan pilih save
#konfigrasi pada file virtualbox.conf
sudo nano virtualbox.conf
mode = gui
machines = cuckoo1
label = cuckoo1
platform = windows
ip = 192.168.46.101
Snapshot 1
#tekan ctrl+x kemudian pilih save
sudo nano processing.conf
```

```
enabled = yes
#tekan ctrl+x kemudian pilih save
#konfigurasi memory.conf
sudo nano memory.conf
guest_profile = Win7SP1x64
#tekan ctrl+x kemudian simpan
vol.py --info |grep Profiles -A48
#lakukan konfigurasi pada reporting.conf
sudo nano reporting.conf
singlefile Enable creation of report.html
enabled = yes
mongodb
enabled = yes
#Tekan ctrl+x kemudian pilih simpan
```

16. Setelah melakukan perintah diatas selanjutnya memanggil *web server cuckoo sanbox* pada operasi sistem *windows* 7 yang sudah terpasang di virtualbox tadi dengan IP *localhost* atau dengan IP *linux ubuntu* tersebut melalui *web browser*.

3.4.1 Menjalankan *Virtual Machine*



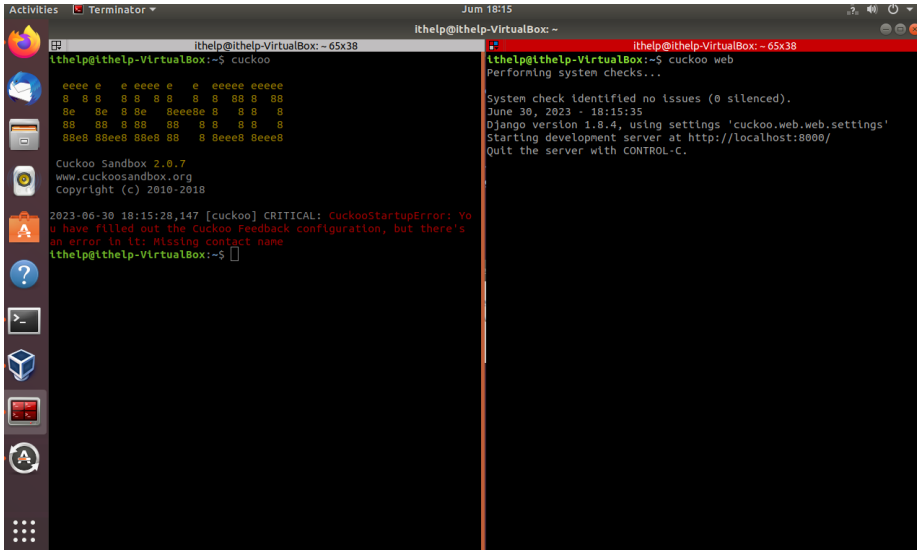
Gambar 3. 23 Proses Installasi Virtualbox
(Sumber Penelitian:2023)

Sebelum memulai Cuckoo, Cuckoo akan memeriksa apakah VirtualBox sudah berjalan. Jika sudah, maka langkah pertama dalam memulai analisis dinamis

adalah menginstal VirtualBox. Dengan menggunakan perintah yang ditunjukkan pada Gambar 3.10, VirtualBox akan dijalankan secara terus menerus; oleh karena itu, tidak perlu untuk memulai mesin virtual sebelum memulai VirtualBox; setelah hal ini dilakukan, Cuckoo dan Cuckoo web dapat dijalankan secara terus menerus.

3.4.2 *Command* pada Cuckoo

Untuk langkah selanjutnya buka tiga terminal dan gunakan perintah cd /opt/Cuckoo/ pada masing-masing terminal. Kemudian, pada terminal, gunakan perintah untuk meluncurkan root cuckoo, web, dan Cuckoo terakhir, menjalankan perintah Cuckoo Rooter. Karena Cuckoo tidak direkomendasikan untuk diluncurkan sebagai root, perintah yang diluncurkan memberikan akses root ke pengguna mana pun yang ditambahkan ke grup Cuckoo tanpa harus meluncurkan Cuckoo sebagai root. Kemudian, setelah peluncuran Cuckoo Rooter, langkah selanjutnya adalah meluncurkan Cuckoo Web pada gambar 3.12, yang berguna untuk menampilkan antarmuka Cuckoo dan memfasilitasi penggunaan Cuckoo Sandbox.. Setelah menjalankan *Cuckoo web*, perintah selanjutnya adalah menjalankan Cuckoo Sandbox agar analisis dapat dilakukan. Gunakan perintah di atas untuk menjalankan Cuckoo untuk mengikuti dan mengamati proses analisis. Setiap tindakan yang dilakukan oleh Cuckoo akan direkam pada terminal.



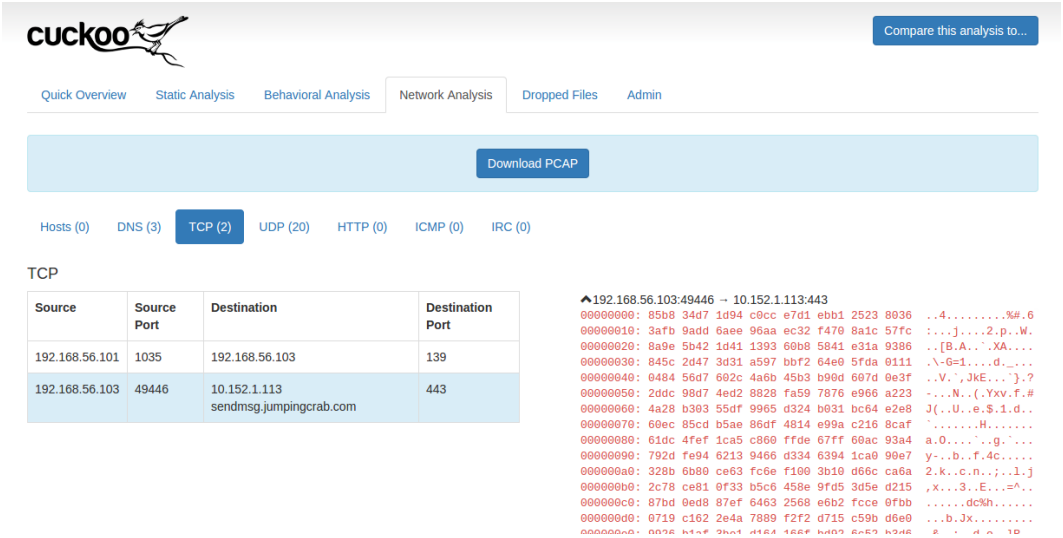
Gambar 3. 24 Menjalankan Cuckoo dan Web Cuckoo
(Sumber Penelitian:2023)

3.4.3 Melakukan Analisis

Setelah semua terminal dijalankan, langkah terakhir adalah mengunggah malware ke web Cuckoo. Cuckoo akan menganalisis secara otomatis dan melaporkan konten apa pun yang bisa diakses di situs webnya Cuckoo gambar 3.24. Ketika ransomware ditambahkan ke Cuckoo, program ini akan melakukan analisis secara otomatis. Namun, sebelum memulai analisis, Cuckoo akan memeriksa apakah VirtualBox sedang berjalan, dan jika semuanya berjalan dengan baik, maka ia akan melakukan analisis melalui *upload web server* 0.0.0.0:8000 /127.0.0.1:8000 pada *browser*.

3.4.4 Laporan

Ketika mensubmit sampel *ransomware, Cuckoo* akan menyediakan hasil akhir seperti gambar () yang dapat diakses kapan saja pada *Cuckoo website*. Laporan dapat di i*mport*, dan disubmit pada komunitas *cuckoo* untuk dokumentasi.



Gambar 3. 25 Laporan Hasil Pengecekan Cuckoo
(Sumber Penelitian:2023)

3.5 Lokasi dan Jadwal Penelitian

Lokasi penelitian dilakukan di PT. NOK Precision Company Batam yang berlokasi di Kawasan Batamindo, Jalan Gaharu Muka Kuning, Batam. Berikut jadwal penelitiannya:

Tabel 3.6 Daftar Jadwal Penelitian

No	Kegiatan	Deskripsi	Tahun 2023					
			Maret	April	Mei	Juni	Juli	Agustus
1	Pengajuan Judul	Pemilihan Judul						
2	Penyusunan Bab I	Identifikasi Masalah						
3	Penyusunan Bab II	Kajian Teori						
4	Penyusunan Bab III	Installasi Sistem						
5	Penyusunan Bab IV	Hasil Analisa						
6	Penyusunan Bab V	Kesimpulan dan saran						
7	Daftar Pustaka,Lampiran							