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.

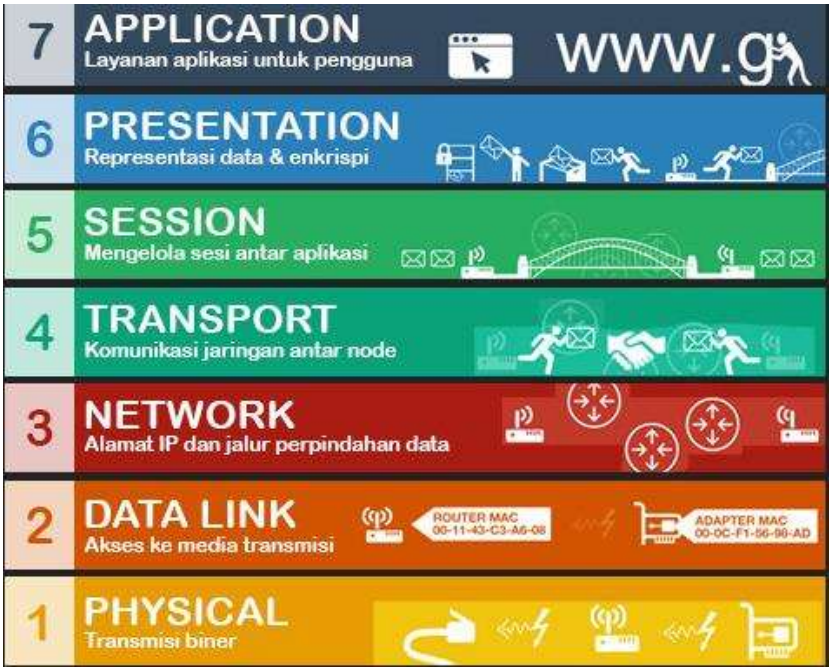
Protokol TCP/IP mendukung berbagai aplikasi seperti email, *browsing web*, transfer file, dan banyak lagi. Hal ini memungkinkan komunikasi yang mulus antara perangkat-perangkat di seluruh jaringan komputer global. Dalam komunikasi

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.

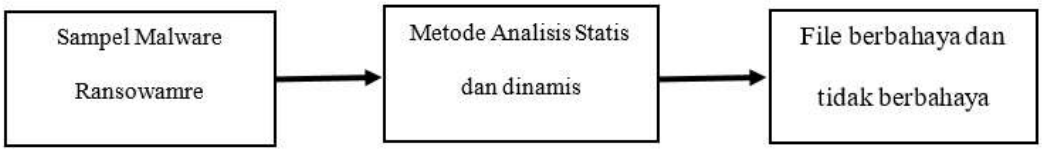
2. Virgiawan A. Manopo,Volume 9 No. 3, ISSN 2301-8402 tahun 2020 dengan judul "Analisa Malware Menggunakan Metode *Dynamic Analysis* Pada Jaringan Universitas Sam Ratulangi". Melakukan penelitian malware *Ransomware* denan metode analisis dinamis dengan tujuan tujuan adalah untuk menganalisa karakteristik 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.