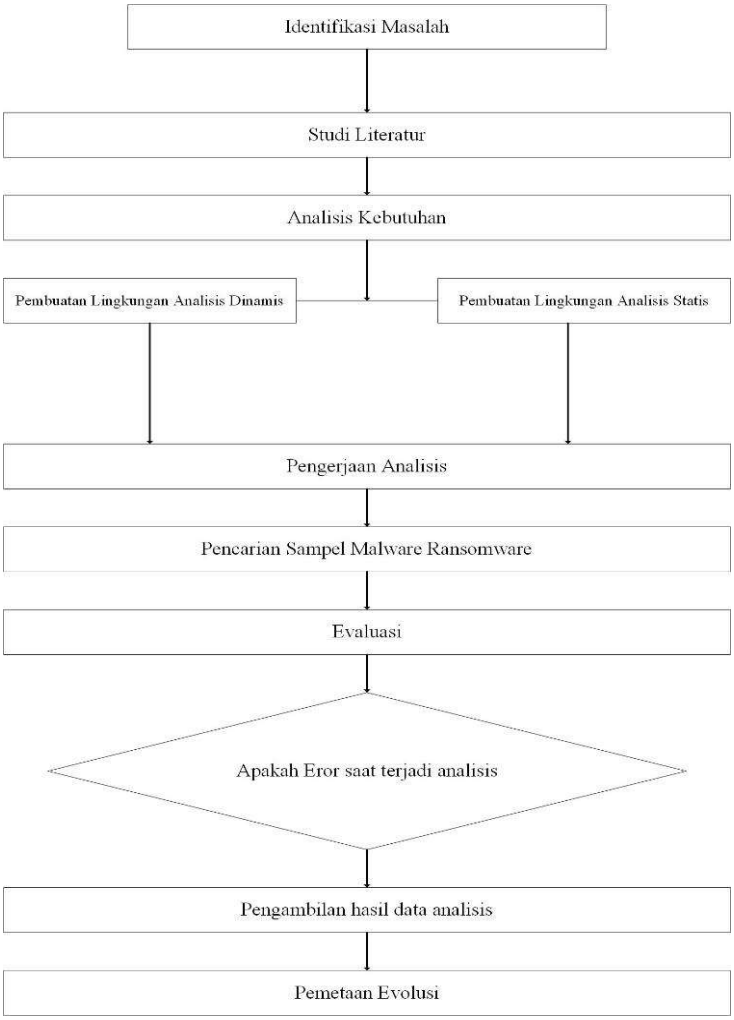
BAB III

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

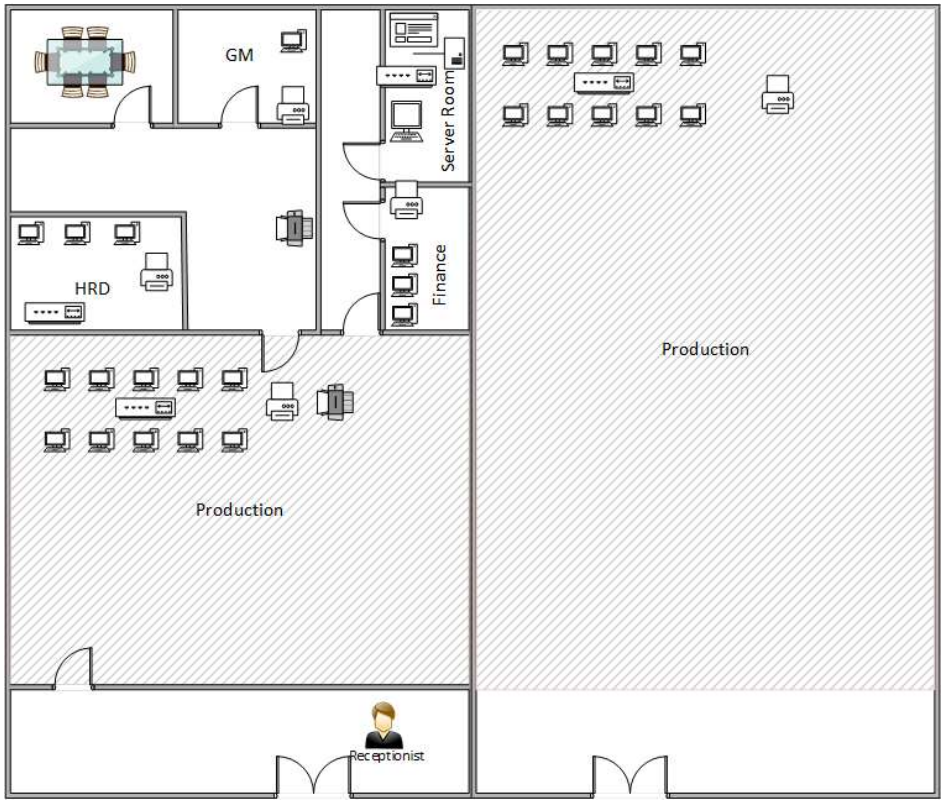
digunakan layanan dedicated 50 Mbps dengan layanan *provider* jasa Batam Bintan Telekomunikasi (BBT). Pada masing-masing client menggunakan windows 10 profesional dan server menggunakan *windows* server 2016. Adapun antivirus yang digunakan adalah AVG *bussiness class*. Berikut tabel analisa *hardware*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



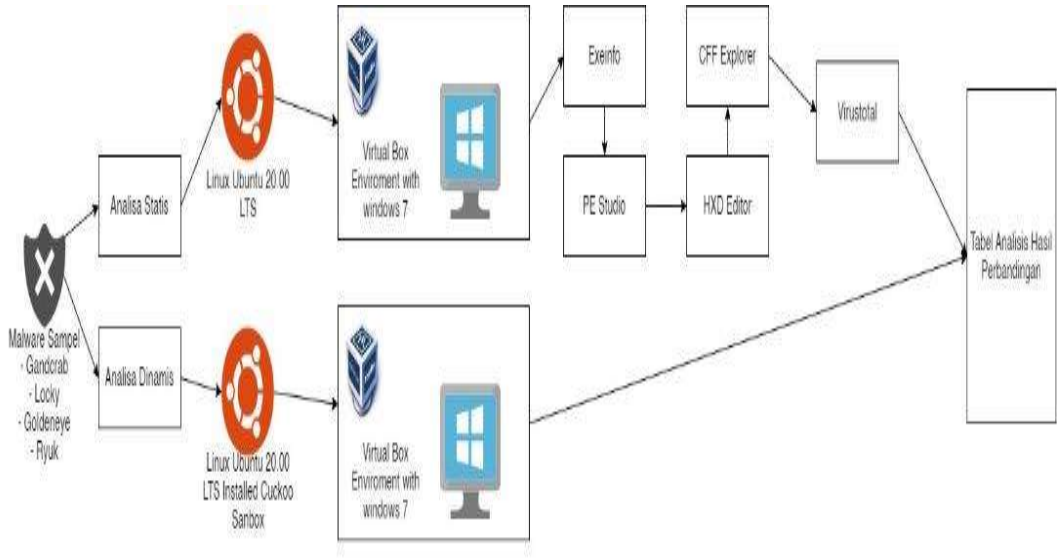
Gambar 3. 2 Topologi jaringan PT. NPCB
(Sumber Penelitian: 2023)

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

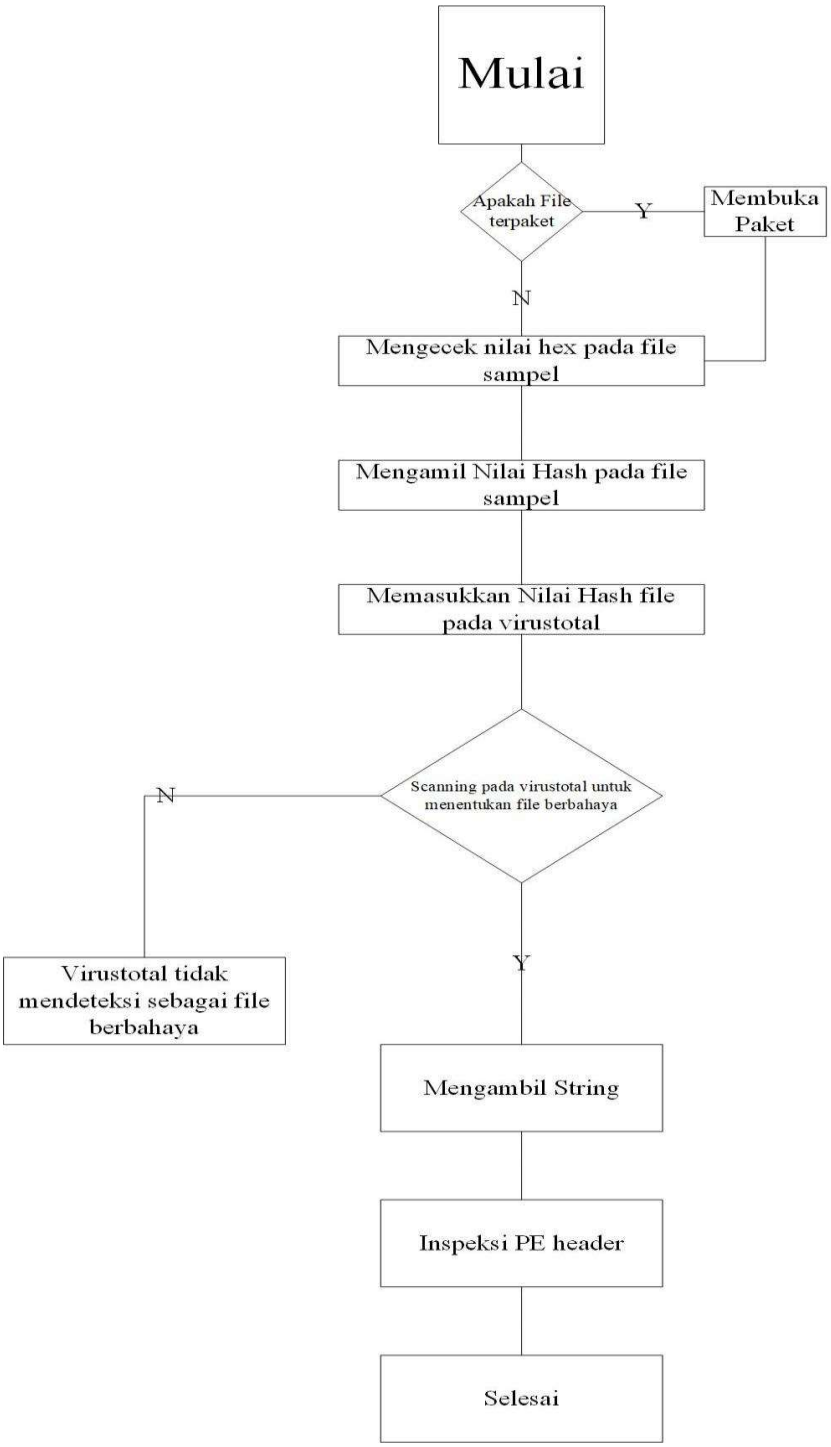
ke lingkungan jaringan PT.NPCB. Berikut topologi dari rancangan analisis keamanan yang akan diterapkan oleh peneliti:



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

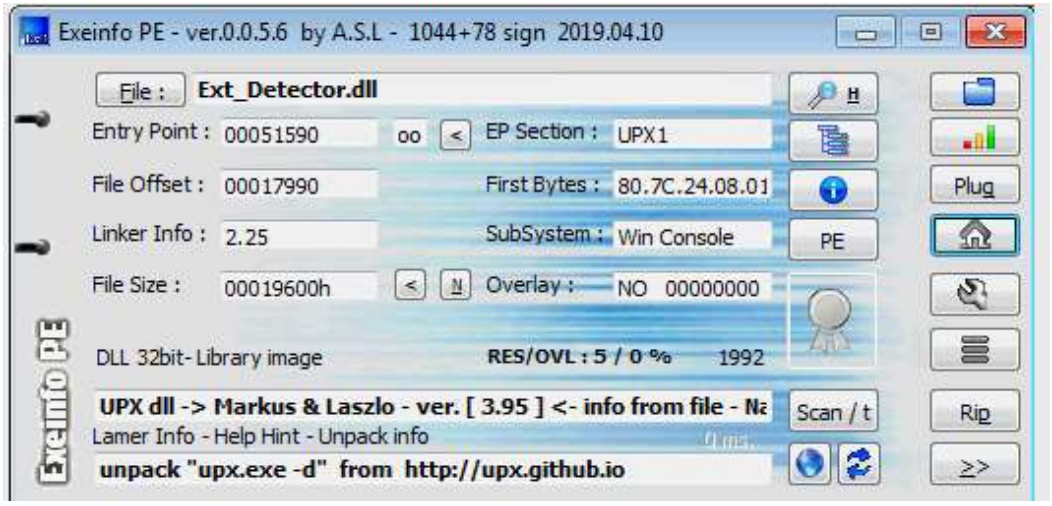
Aplikasi	Sumber	Operasi Sistem
PE Studio	https://www.winitor.com/download	Windows 7
CFF Explorer	https://github.com/cybertechniques/site/blob/master/analysis_tools/cff-explorer/index.md	Windows 7
Hxd Editor	https://mh-nexus.de/en/hxd/	Windows 7
Virustotal	https://www.virustotal.com/	Windows 7

3.3.3 Analisis jenis file terdapat paket

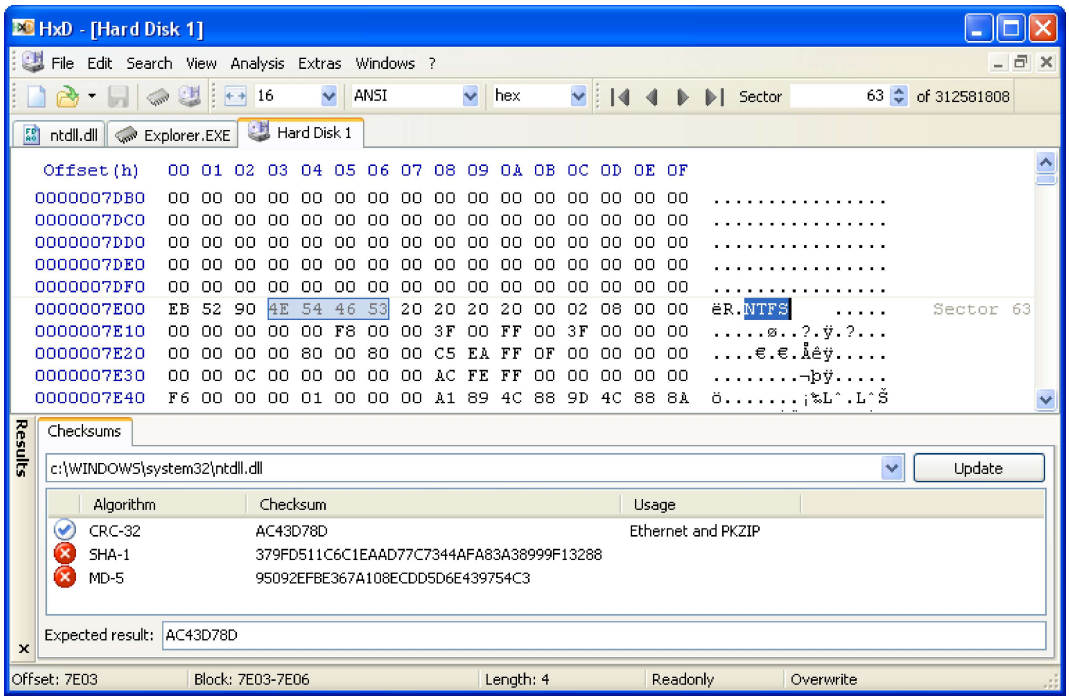
Biasanya, *ransomware* didistribusikan dalam bentuk paket. Paket ini memiliki kemampuan untuk menghapus *ransomware* dari file asli, membuatnya tampak seperti perangkat lunak yang aman. Jika *ransomware* sudah dipaketkan, file yang bersangkutan tidak dapat diperiksa dengan cermat, dan jika *ransomware*

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)

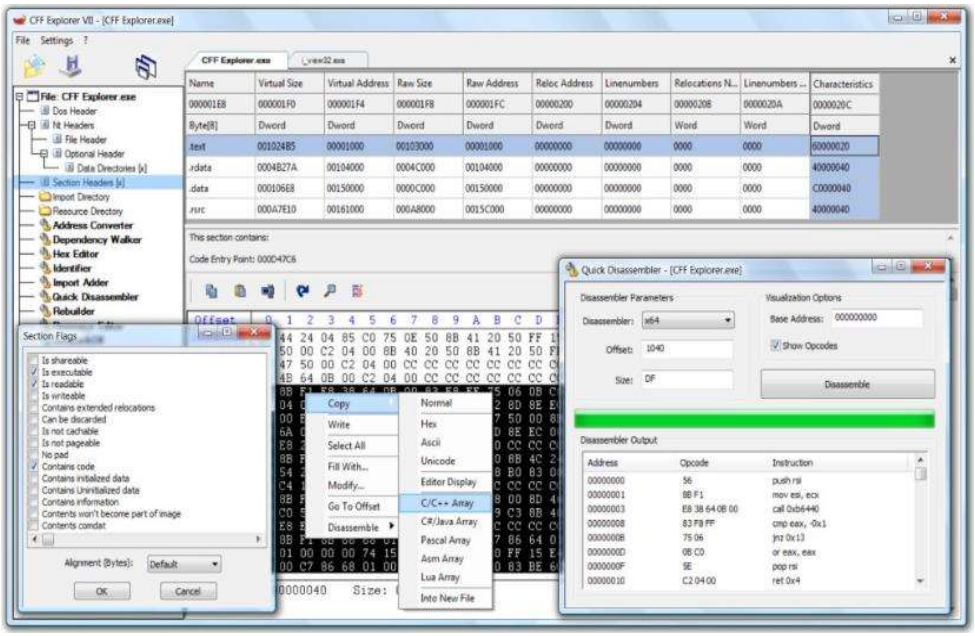
Pada gambar 3.6, ditampilkan metode manual untuk memahami jenis file. Ada banyak metode yang dapat digunakan untuk menentukan jenis file, termasuk CFFexplorer, PE32, dan Python. Dari hasil alat manual HxD, contoh cara memahami dasar-dasar jenis file adalah dengan melihat nilai awal 2 bit dari kode heksadesimal 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.

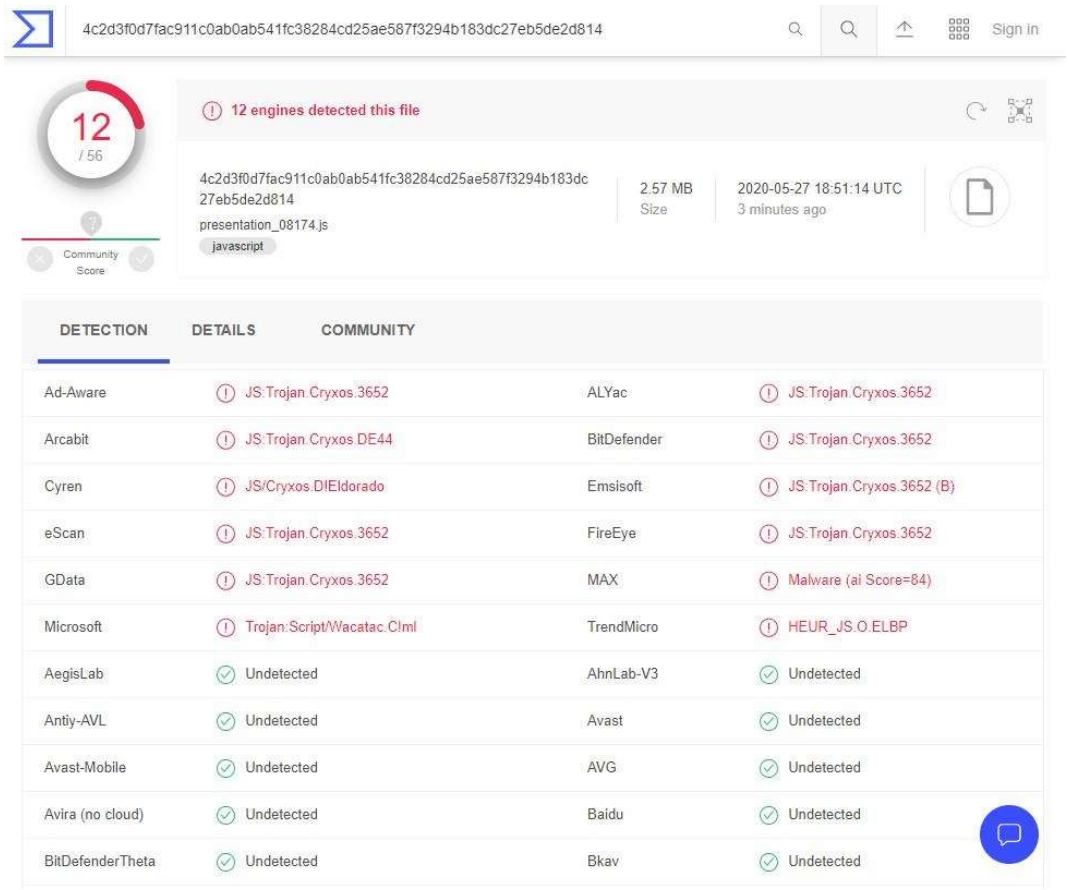
Nilai hash dapat dibuat menggunakan CFFexplorer atau PeStudio, dan kemudian akan diunggah ke situs *web* VirusTotal untuk mengumpulkan informasi yang *komprehensif*.



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.



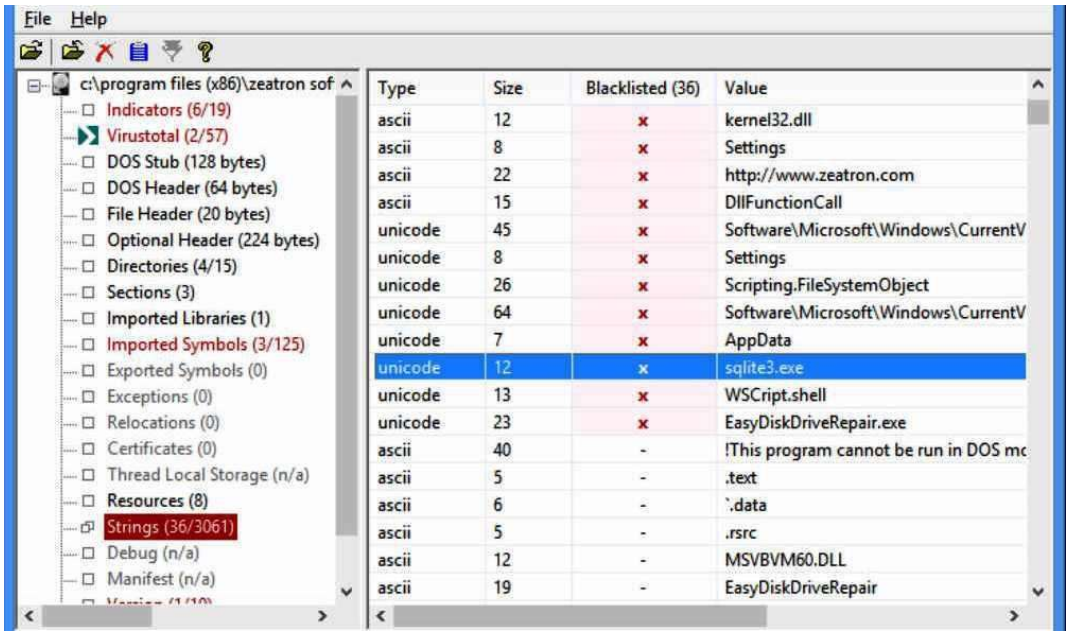
Gambar 3. 8 Tampilan Proses Virustotal
(Sumber Penelitian:2023)

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.

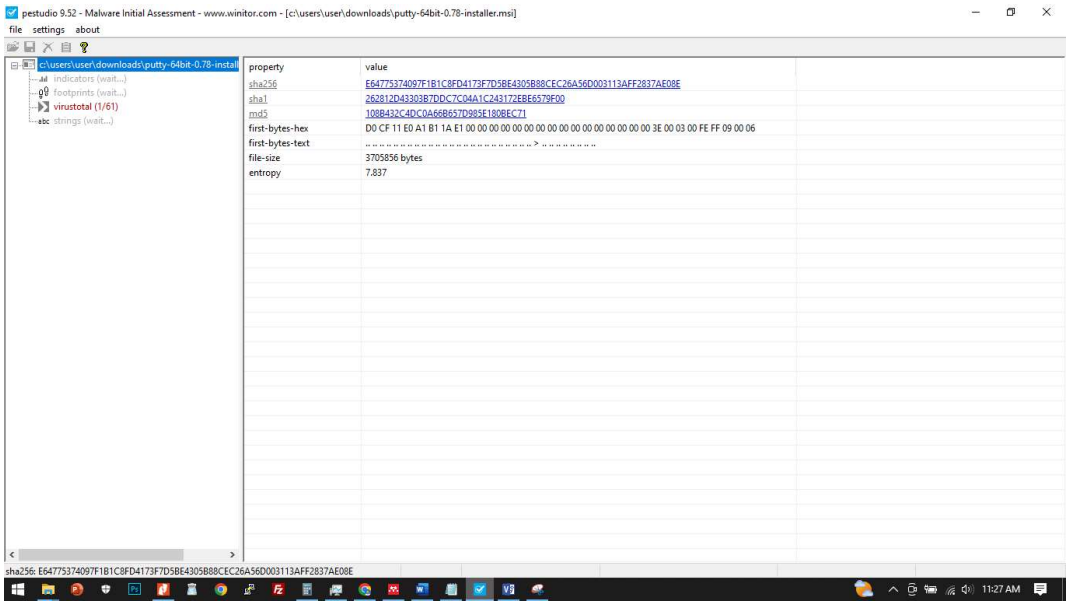
3.3.7 Inspeksi PE *Header*

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)

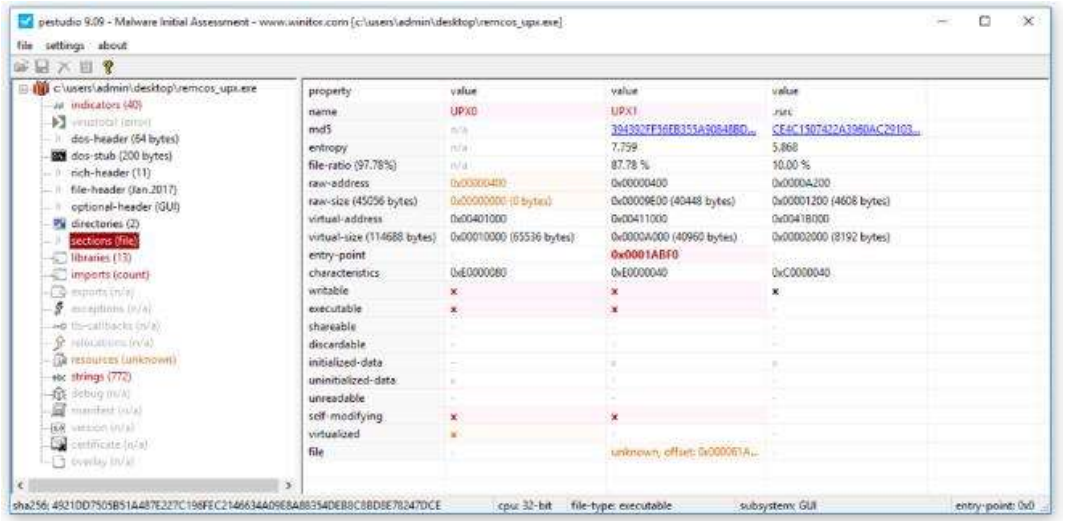
Dapat dilihat dalam tabel diatas penjelasan bagian bagian PE *header* dan pada bagian section disebutkan tentang data yang akan di jelaskan pada tabel di bawah:

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.

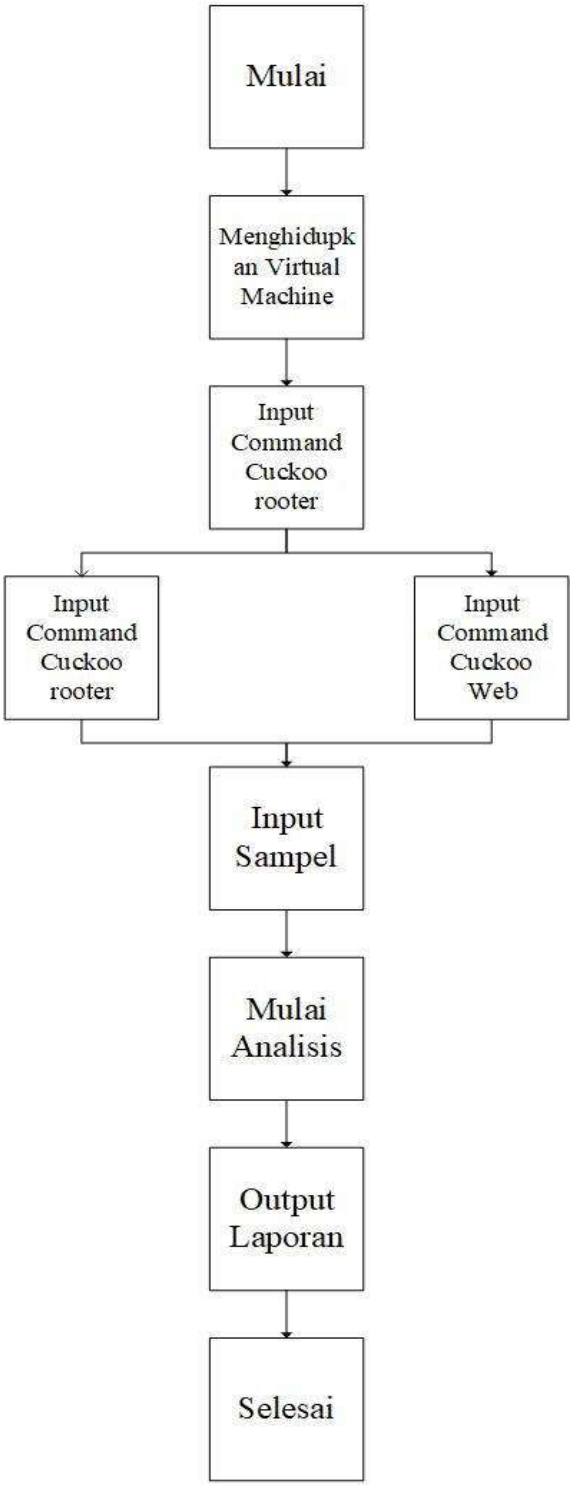


Gambar 3. 11 Tampilan Section pada PE Studio
(Sumber Penelitian:2023)

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

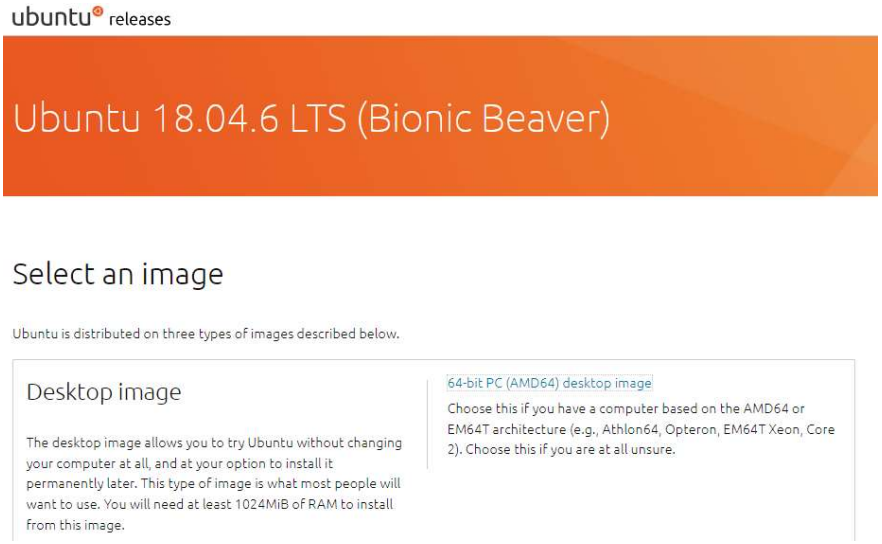
Berikut daftar kebutuhan *hardware* dan *software* yang dibutuhkan penulis untuk analisa dinamis:

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

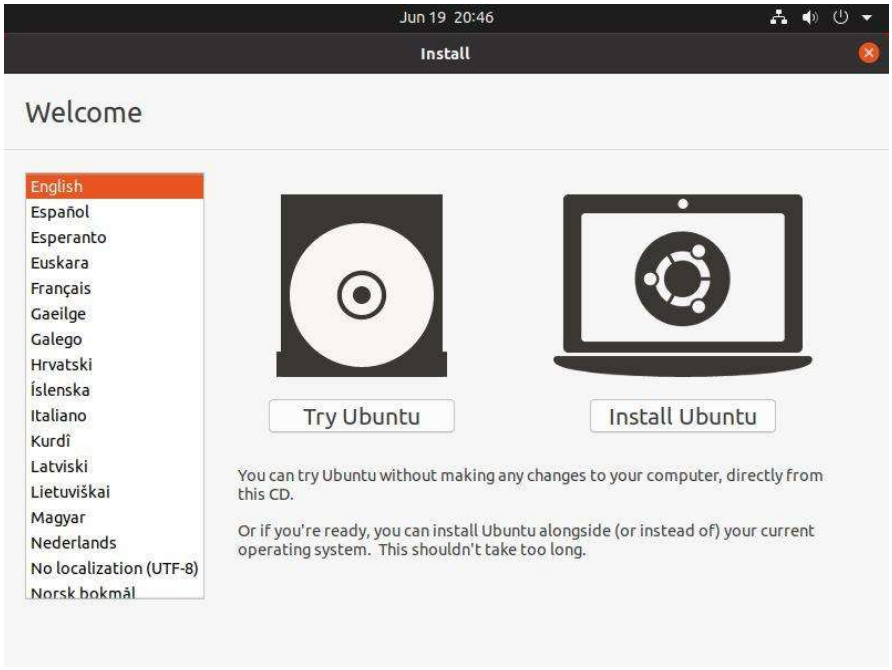
Pada proses penelitian analisis *malware* metode dinamis menggunakan *cuckoo sanbox* yang ditanamkan pada *Linux Ubuntu* berikut proses installasi sistem tersebut:

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

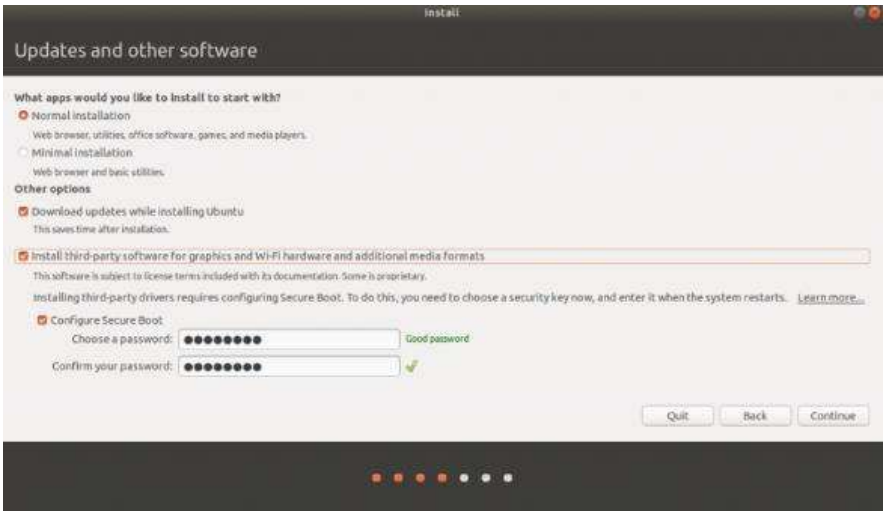


Gambar 3. 13 Download Iso Image Ubuntu 18.04 LTS(Focal Fossa)
(Sumber Penelitian:2023)

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

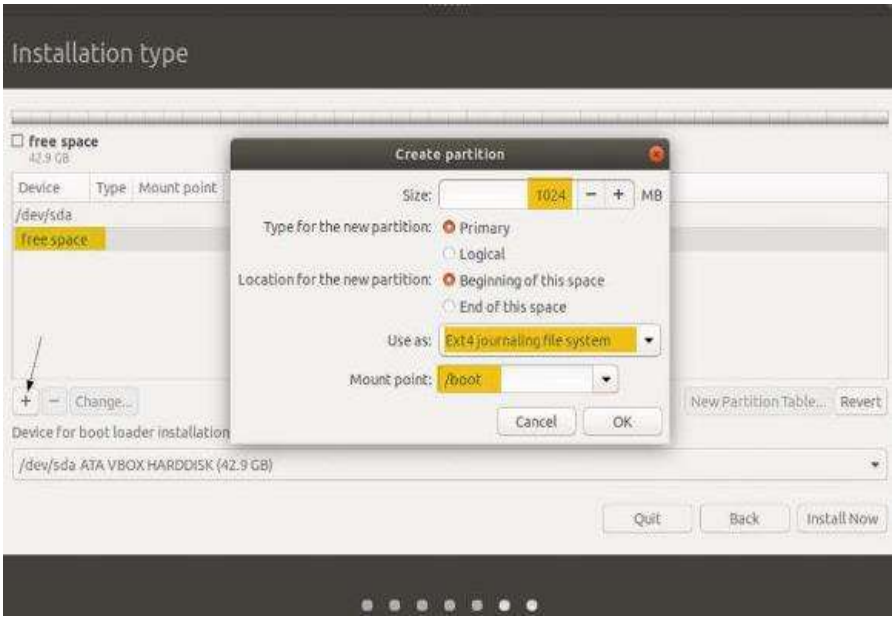


Gambar 3. 14 Proses Installasi Ubuntu
(Sumber Penelitian:2023)



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

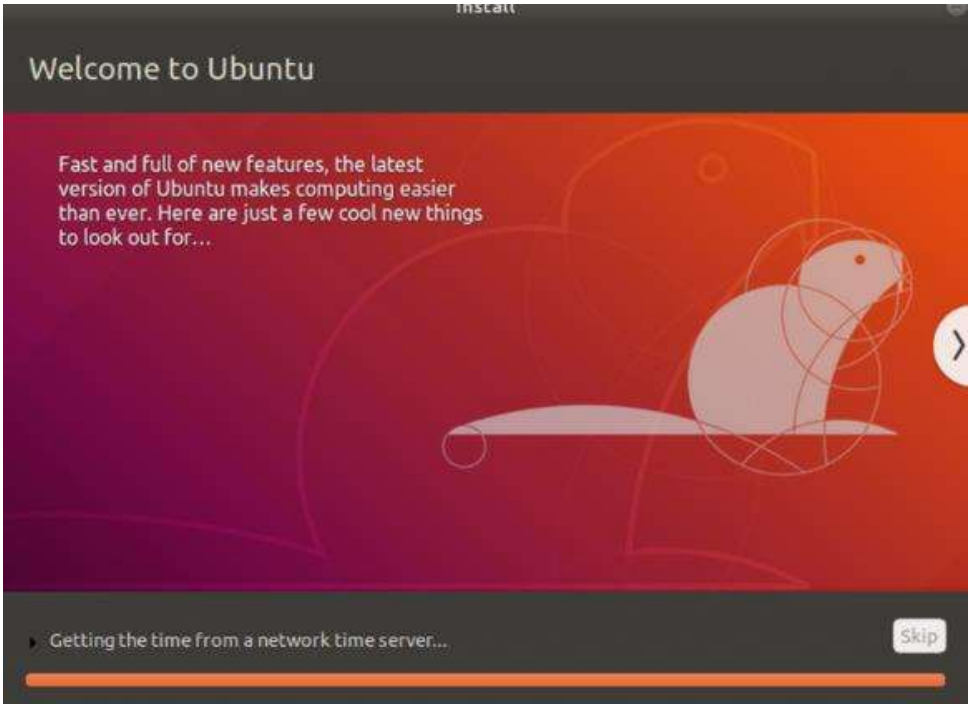
3. Melakukan pemilihan installasi *linux* dengan *other options* agar *linux* mendapatkan *update driver hardware,* dan *tools default* tambahan.



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)

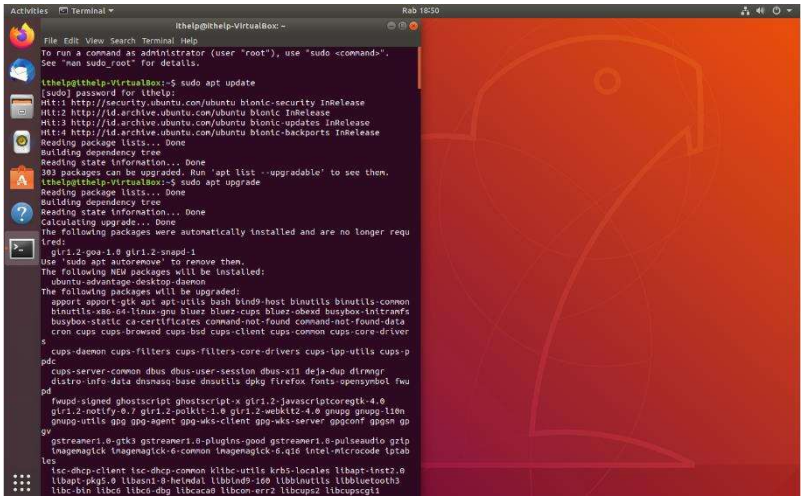
6. Setelah melakukan installasi *linux* operasi sistem lakukan *update* pada *repository linux* dengan *command* seperti berikut:

```
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
```



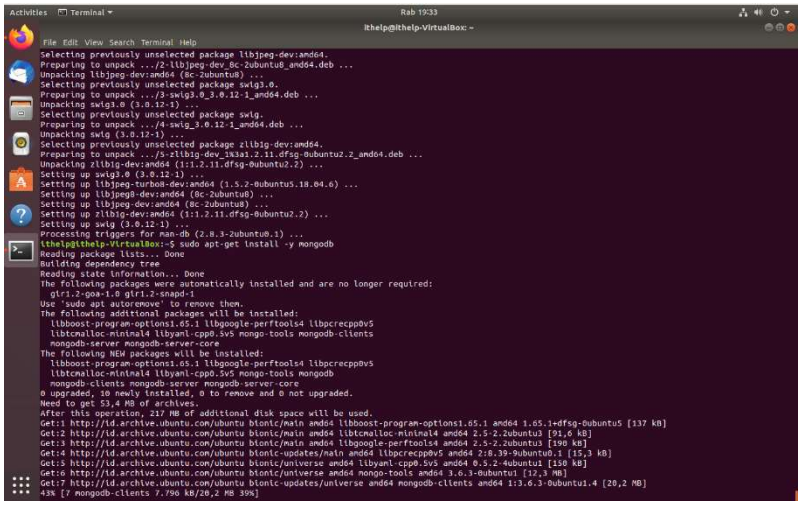
Gambar 3. 18 Proses Upgrade dan Update Reposiroty Linux
(Sumber Penelitian:2023)

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 ..
```

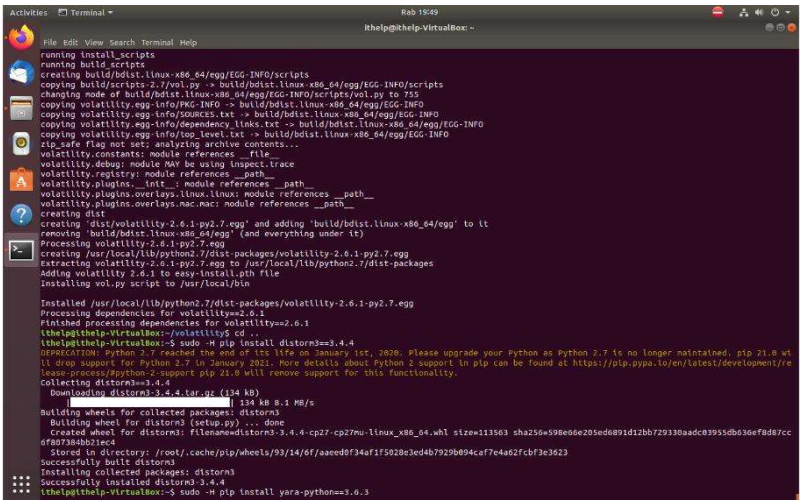
Gambar 3. 20 Download Virtualbox
(Sumber Penelitian:2023)

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
```

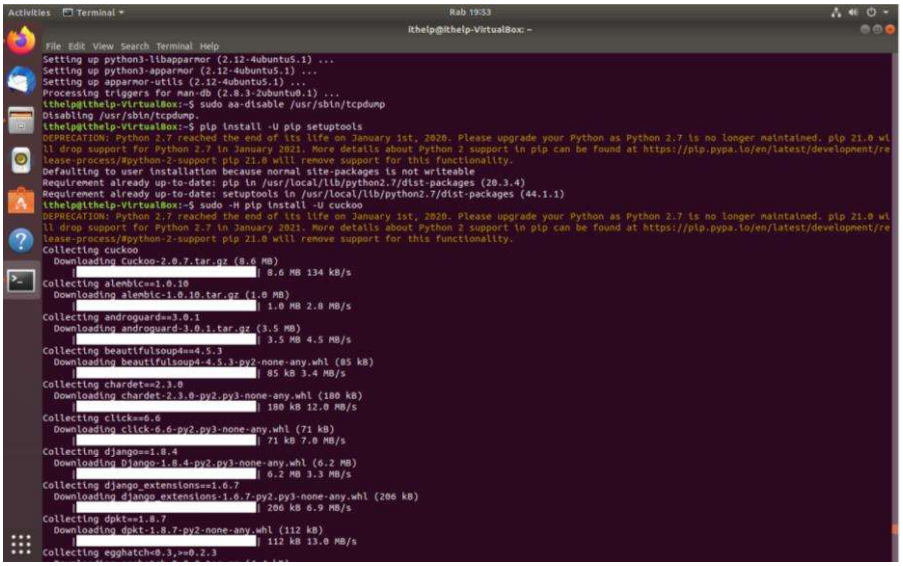


Gambar 3. 21 Installasi library python
(Sumber Penelitian:2023)

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*,

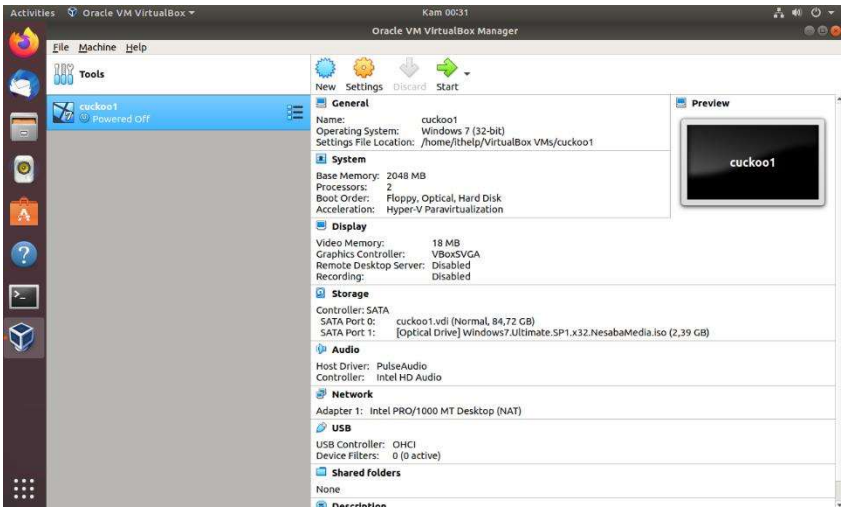
```
sudo apt-get install -y iptables-persistent
sudo iptables -A FORWARD -o eth0 -i vboxnet0 -s
192.168.56.0/24 -m conntrack --ctstate NEW -j ACCEPT

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*



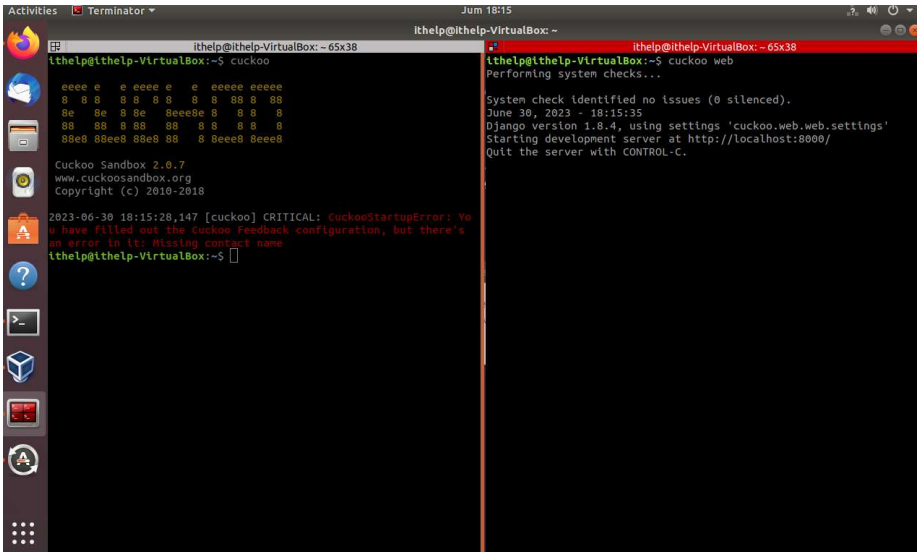
Gambar 3. 23 Proses Installasi Virtualbox
(Sumber Penelitian:2023)

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.



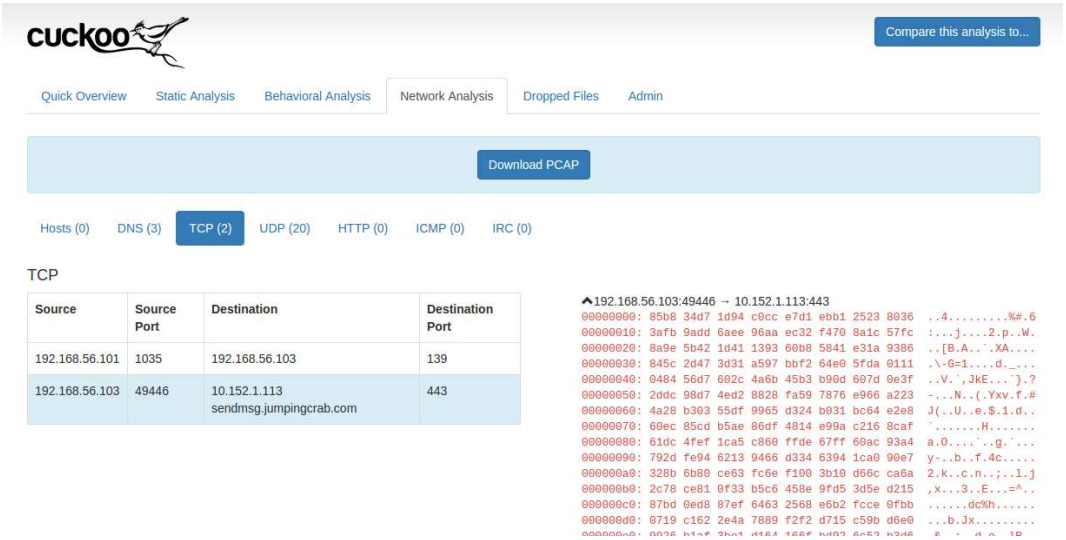
Gambar 3. 24 Menjalankan Cuckoo dan Web Cuckoo
(Sumber Penelitian:2023)

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							