

Buku Panduan

SISTEM ANALISIS MALWARE BERBASIS MACHINE
LEARNING PADA LINGKUNGAN AIRGAP
MENGUNAKAN MINI-PC (AIRMALYSIS)

OLEH: ATANASIUS PRADIPTHA SAMPURNO || KINANTI ARIA WIDASWARA || TRI MULIA BAHAR

Daftar Isi

Daftar Isi	i
Pendahuluan.....	1
1. Tujuan	1
2. Cakupan	1
3. Target Pengguna.....	1
4. Spesifikasi Sistem	1
5. Riwayat Dokumen	2
Instalasi	3
1. Konfigurasi <i>User</i> Linux	3
2. Unduh Cuckoo3	3
3. Instalasi Cuckoo3.....	3
4. Tes Cuckoo3.....	4
5. Unduh Aplikasi Sistem	5
Panduan Penggunaan Aplikasi.....	6
1. Panduan Umum Menggunakan Aplikasi	6
a. Menyalakan Aplikasi	6
b. Proses <i>Setup</i>	7
c. Unggah File.....	7
d. Proses Analisis	9
e. Status Analisis.....	9
f. Laporan Singkat	9
g. Laporan PDF	10
h. Analisa Ulang.....	11

Pendahuluan

1. Tujuan

Buku panduan ini dirancang untuk memberikan gambaran dan petunjuk dalam menggunakan aplikasi Sistem Analisis Malware Berbasis Machine Learning Pada Lingkungan Airgap Menggunakan Mini-PC. Panduan ini bertujuan untuk membantu pengguna dalam memahami fungsi dan fitur utama sistem analisis ini. Dengan adanya buku panduan ini, pengguna diharapkan dapat memahami cara kerja sistem sehingga dapat menggunakan secara optimal.

2. Cakupan

Panduan ini mencakup spesifikasi, proses instalasi, dan penggunaan fitur utama aplikasi. Fitur yang dijelaskan meliputi proses setup, unggah data, pembuatan laporan singkat, laporan detil, serta analisis ulang. Panduan ini tidak memuat integrasi *source-code* melainkan hanya penggunaan aplikasi secara umum.

3. Target Pengguna

Buku panduan ini ditujukan untuk pihak yang terlibat di bidang keamanan siber dan analisis *malware*. Panduan ini relevan bagi pengguna yang akan menggunakan Sistem Analisis Malware Berbasis Machine Learning Pada Lingkungan Airgap Menggunakan Mini-PC. Dengan penjelasan yang ringkas dan sistematis, buku ini membantu pengguna memahami fitur serta alur kerja sistem secara menyeluruh.

4. Spesifikasi Sistem

Sebelum menggunakan sistem analisis ini, pastikan perangkat komputer yang digunakan **harus** sesuai dengan spesifikasi berikut:

Komponen	Nama	Versi
Host	Linux	-
Sistem Operasi	Ubuntu	22.04
Bahasa Pemrograman	Python	3.10

5. Riwayat Dokumen

Versi	Tanggal	Pemilik Aplikasi	Deskripsi
1.0	17 Juli 2025	Pengembang Sistem	Rilis Awal

Instalasi

Bagian ini akan memuat instalasi *sandbox* cuckoo3. Bagian ini bagian terpenting dalam penggunaan aplikasi ini. Adapun langkah untuk instalasi *cuckoo3* adalah sebagai berikut:

1. Konfigurasi User Linux

Pastikan nama *user* perangkat bernama “cuckoo”. Apabila nama *user* menggunakan nama yang lain, Anda wajib membuat *user* baru dengan menggunakan perintah:

```
sudo adduser cuckoo
```

Setelah itu, Anda dapat berpindah ke *user* cuckoo tersebut baik menggunakan fitur *switch user* atau dengan perintah:

```
su cuckoo
```

Apabila nama *user* sudah *cuckoo*, Anda dapat melewati tahapan ini.

2. Unduh Cuckoo3

Unduh cuckoo3 pada link berikut ini:

```
https://cuckoo-hatch.cert.ee/static/docs/
```

3. Instalasi Cuckoo3

Selesaikan seluruh proses *installing* dan *configuring* hingga tahap Web API. Bagian *Network Routing* tidak perlu diselesaikan. Setelah selesai, buka file `web_local_settings.py` dengan menggunakan perintah:

```
nano ~/.cuckoocwd/web/web_local_settings.py
```

Setelah itu, ubah `DEBUG = false` menjadi `DEBUG = true`. Perubahan ini akan memastikan bahwa antarmuka halaman web Cuckoo3 tampil dengan baik dan dapat digunakan sebagaimana mestinya. **Pastikan Anda tidak mengubah alamat IP apapun.**

4. Tes Cuckoo3

Untuk memastikan cuckoo3 sudah terunduh dengan sempurna, Anda dapat melakukan pengecekan secara manual dengan melakukan hal berikut:

1. Buka terminal
2. Pindah ke direktori cuckoo3 dengan menggunakan perintah:

```
cd cuckoo3
```

3. Nyalakan *virtual environment* dengan menggunakan perintah:

```
source venv/bin/activate
```

4. Jalankan perintah perintah berikut:

```
cuckoo
```

5. Ulangi langkah 1-3.

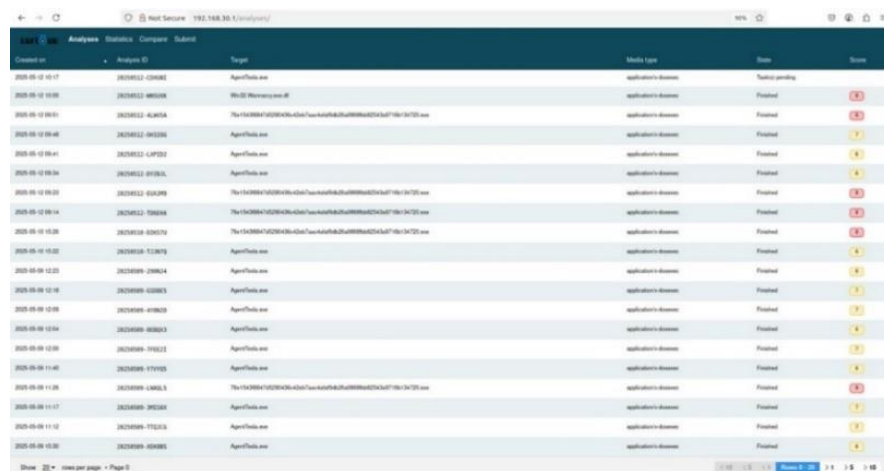
6. Jalankan langkah berikut:

```
cuckoo web --host 127.0.0.1 --port 8000
```

7. Buka *web browser* dan pada *search bar* ketik halaman web berikut:

```
127.0.0.1:8000
```

8. Apabila cuckoo3 sudah terinstall dengan benar, tampilan web seharusnya sebagai berikut:



Target	Analysis ID	Target	Malware Type	Status	Score
2025-05-12 10:17	20250512-101802	Agent/Cuckoo.exe	Application/Document	Finished	
2025-05-12 10:18	20250512-101808	Win32/Word.Document.12	Application/Document	Finished	3.5
2025-05-12 10:19	20250512-101814	Thy13a388a7c0284b3e42a77aee4a4a8b23a4888a4d23a4a77b1b73a72b.exe	Application/Document	Finished	3.5
2025-05-12 10:40	20250512-101820	Agent/Cuckoo.exe	Application/Document	Finished	3.5
2025-05-12 10:41	20250512-101826	Agent/Cuckoo.exe	Application/Document	Finished	3.5
2025-05-12 10:54	20250512-101832	Agent/Cuckoo.exe	Application/Document	Finished	3.5
2025-05-12 10:55	20250512-101838	Thy13a388a7c0284b3e42a77aee4a4a8b23a4888a4d23a4a77b1b73a72b.exe	Application/Document	Finished	3.5
2025-05-12 10:56	20250512-101844	Thy13a388a7c0284b3e42a77aee4a4a8b23a4888a4d23a4a77b1b73a72b.exe	Application/Document	Finished	3.5
2025-05-12 10:57	20250512-101850	Thy13a388a7c0284b3e42a77aee4a4a8b23a4888a4d23a4a77b1b73a72b.exe	Application/Document	Finished	3.5
2025-05-12 10:58	20250512-101856	Thy13a388a7c0284b3e42a77aee4a4a8b23a4888a4d23a4a77b1b73a72b.exe	Application/Document	Finished	3.5
2025-05-12 10:59	20250512-101902	Agent/Cuckoo.exe	Application/Document	Finished	3.5
2025-05-12 11:00	20250512-101908	Agent/Cuckoo.exe	Application/Document	Finished	3.5
2025-05-12 11:01	20250512-101914	Thy13a388a7c0284b3e42a77aee4a4a8b23a4888a4d23a4a77b1b73a72b.exe	Application/Document	Finished	3.5
2025-05-12 11:02	20250512-101920	Thy13a388a7c0284b3e42a77aee4a4a8b23a4888a4d23a4a77b1b73a72b.exe	Application/Document	Finished	3.5
2025-05-12 11:03	20250512-101926	Agent/Cuckoo.exe	Application/Document	Finished	3.5
2025-05-12 11:04	20250512-101932	Agent/Cuckoo.exe	Application/Document	Finished	3.5
2025-05-12 11:05	20250512-101938	Agent/Cuckoo.exe	Application/Document	Finished	3.5
2025-05-12 11:06	20250512-101944	Agent/Cuckoo.exe	Application/Document	Finished	3.5
2025-05-12 11:07	20250512-101950	Agent/Cuckoo.exe	Application/Document	Finished	3.5
2025-05-12 11:08	20250512-101956	Thy13a388a7c0284b3e42a77aee4a4a8b23a4888a4d23a4a77b1b73a72b.exe	Application/Document	Finished	3.5
2025-05-12 11:09	20250512-102002	Agent/Cuckoo.exe	Application/Document	Finished	3.5
2025-05-12 11:10	20250512-102008	Agent/Cuckoo.exe	Application/Document	Finished	3.5
2025-05-12 11:11	20250512-102014	Agent/Cuckoo.exe	Application/Document	Finished	3.5
2025-05-12 11:12	20250512-102020	Agent/Cuckoo.exe	Application/Document	Finished	3.5
2025-05-12 11:13	20250512-102026	Agent/Cuckoo.exe	Application/Document	Finished	3.5
2025-05-12 11:14	20250512-102032	Agent/Cuckoo.exe	Application/Document	Finished	3.5

9. Untuk memastikan perintah unggah file dapat diunggah, Anda dapat mengulangi langkah 1-3, lalu jalankan perintah berikut:

```
cuckoo submit [direktori sampel malware]
```

10. Apabila fitur cuckoo submit berjalan sempurna dan proses analisis dijalankan oleh cuckoo, Anda telah berhasil mengintalasi cuckoo3.

5. Unduh Aplikasi Sistem

Setelah instalasi cuckoo3, langkah selanjutnya adalah pengunduhan aplikasi. Unduh aplikasi sistem analisis *malware* dengan menggunakan perintah berikut:

```
git clone https://github.com/atanasiusps/TA_AnalisisMalware
```

Panduan Penggunaan Aplikasi

1. Panduan Umum Menggunakan Aplikasi

Bagian ini memuat petunjuk dasar dalam menggunakan sistem analisis malware berbasis machine learning pada lingkungan airgap. Panduan mencakup prosedur menjalankan sistem dan menggunakan fitur-fitur utama yang tersedia. Panduan ini tidak akan mencakup konfigurasi *virtual machine* ataupun konfigurasi di luar dokumentasi resmi cuckoo3. Adapun panduan penggunaan aplikasi adalah sebagai berikut:

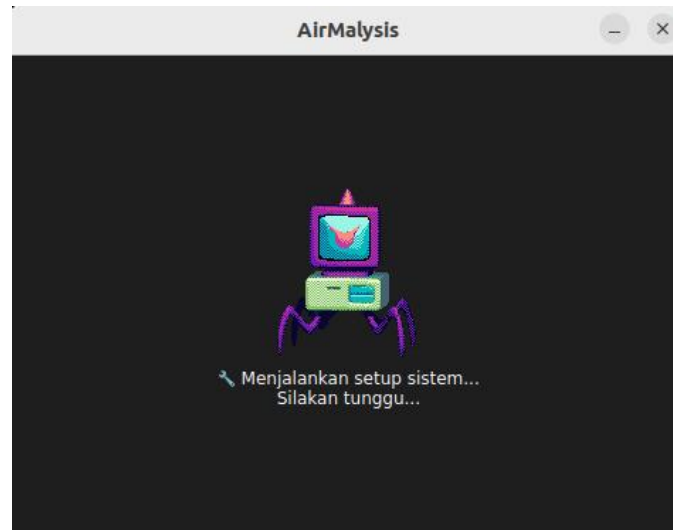
a. Menyalakan Aplikasi

Untuk menjalankan aplikasi, pengguna dapat menekan ikon aplikasi. Ikon ini digunakan untuk mempermudah penjalanan aplikasi tanpa harus menggunakan *Command Line Interface* (CLI). Berikut gambar ikon aplikasi AirMalSys:



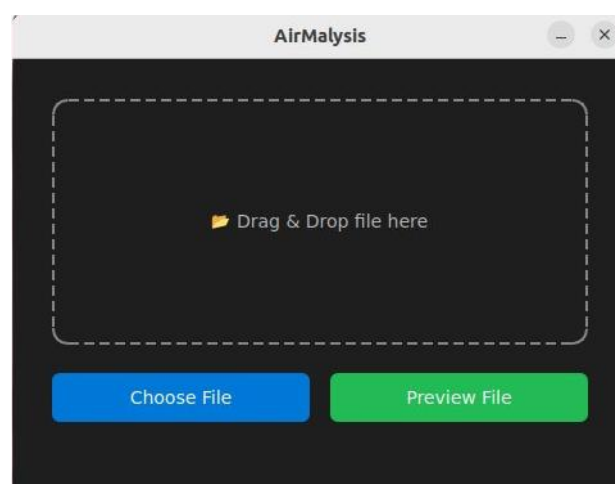
b. Proses Setup

Setelah aplikasi dijalankan, maka sistem akan melakukan *setup*, yaitu dengan mengaktifasi *sandbox* dan web *localhost* cuckoo3. Selain itu, aplikasi juga akan mengaktifkan modul-modul aplikasi. Berikut merupakan tampilan antarmukanya:

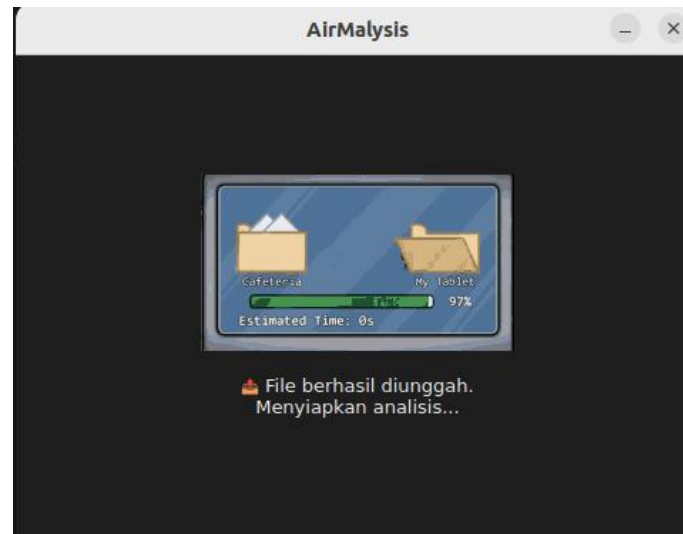


c. Unggah File

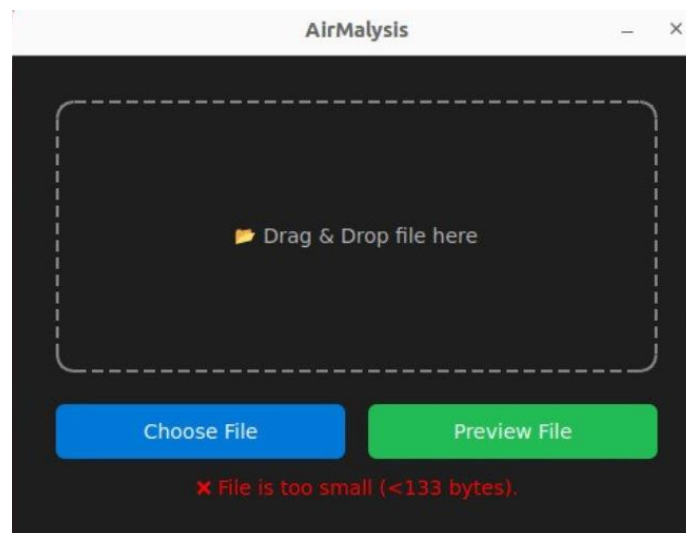
Setelah proses *setup* selesai, maka akan ditampilkan modul antarmuka untuk mengunggah *file* yang diinginkan. Terdapat dua metode untuk melakukan pengunggahan, yang pertama itu menggunakan fitur *drag and drop*, atau dapat dilakukan juga dengan memilih file secara manual. Berikut merupakan antarmuka modul unggah:



Apabila *file* yang ingin dianalisis berhasil diunggah ke cuckoo3, berikut merupakan tampilannya:

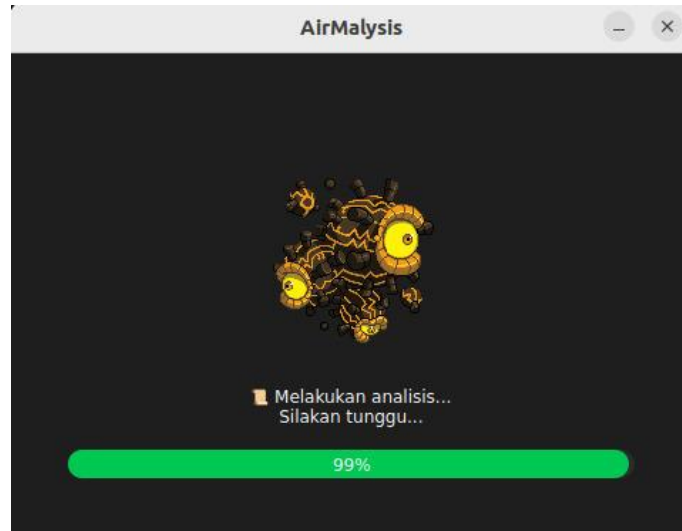


Tidak semua *file* dapat diunggah ke dalam cuckoo3. Terkadang pengunggahan dapat gagal. Beberapa alasan seperti ukuran *file* terlalu kecil, *file* kosong, ekstensi *file* tidak compatible, dan sebagainya menjadi faktor kegagalan. Apabila file yang ingin dianalisis gagal diunggah ke cuckoo3, berikut merupakan tampilannya:



d. Proses Analisis

Setelah *file* selesai divalidasi, maka *file* akan diunggah ke *sandbox* cuckoo3. Berikut merupakan tampilan antarmukanya:

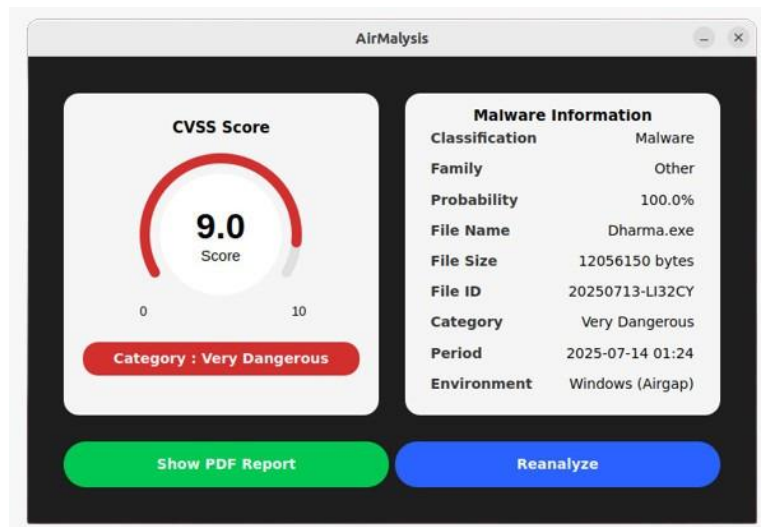


e. Status Analisis

Apabila *file* yang diunggah berhasil dianalisis, maka aplikasi akan memunculkan laporan singkat. Apabila gagal, maka aplikasi akan kembali ke halaman unggah. Setelah itu, pengguna diharapkan dapat mengunggah *file* lainnya.

f. Laporan Singkat

Setelah proses analisis telah selesai, maka akan ditampilkan. Laporan akan menampilkan beberapa informasi penting bagi pengguna. Informasi yang ditampilkan adalah skor perilaku malware, klasifikasi, *family*, probabilitas, nama *file*, ukuran *file*, *task* ID, kategori, waktu, dan lingkungan. Setelah itu, pengguna dapat membuka laporan PDF untuk laporan yang lebih detail. Berikut merupakan tampilan antarmukanya:



g. Laporan PDF

Pengguna dapat membuka laporan PDF untuk laporan yang lebih detail. Bagian atas laporan berisi informasi mengenai *file* yang diunggah. Setelah itu, laporan ini memberikan informasi mengenai perilaku *malware* pada bagian “*Detected Signatures*”. Laporan juga berisi glosarium untuk istilah-istilah teknis dan pengertiannya.

Malware Analysis Report

Created on: 2025-07-11

Analysis Summary

Analysis ID	20250711-VYIBV5
File Name	7ev3n.exe
File Size	322560
MD5	9f8bc96c96d43ecb69f883388d228754
SHA256	7d373ccb86d1dbb1856cf31afa87c2112a0c1795a796ab01cb154700288afec5
Start Time	2025-07-11 11:15:52 WIB
End Time	2025-07-11 11:18:08 WIB
Severity Score	9.0 (Critical)
Classification	Malware (Confidence: 100.0%)
Malware Family	Other

Detected Signatures

No.	Signature Name	Description
1	wrote_proc_memory	A process wrote data to an area of memory in another process.
2	executes_dropped_exe	A process was created using a dropped executable.
3	process_other_parent	Created a process with a different parent than the creating process.
4	susevont_adjustprivilegetoken	A privilege for an access token was adjusted. Windows uses the token to control the ability of the user to perform various system-related operations.
5	files_drops_exe_user	Drops file in user directory
6	files_drops_exe_general	Drops executable file
7	cmd_schtasks_create	Uses schtasks.exe to create a new scheduled task.
8	registry_write_runkey	Adds run entry to the registry to gain persistence across system reboots.
9	registry_winlogon_persistence	Modifies WinLogon for persistence
10	registry_bypasses_uac	Modifies registry value(s) to disable UAC checks.
11	file_drops_windows	Drops file in Windows directory

h. Analisa Ulang

Pengguna dapat menekan tombol “Re-Analyze” untuk melakukan analisis lagi untuk *file* lainnya. Tampilan antarmuka analisa ulang akan sama seperti tampilan unggah *file* pada awal.

